Comprehensive IT Service Level Agreement

in Direct Support of the MNsure Business Operations

Effective Date: February 6, 2015

Version 3.2

Table of Contents

Introduction

Service Level Agreement

A service level agreement is a negotiated agreement that records the common understanding about services, priorities, responsibilities, guarantees and warranties between two parties, where one is the customer and the other is the service provider. The purpose of the Comprehensive IT Service Level Agreement (Agreement or SLA) is to spell out the relationship and expectations of the consolidated executive branch IT organization – the Office of MN.IT Services – and each of its individual executive branch agency customers.

Documenting a Cooperative Relationship

The SLA is, by nature and intent, the articulation of a vital cooperative relationship between information technology and the state government business that it serves. It is a living document that serves as a tool for defining expectations, roles and responsibilities, processes and procedures that will help the very diverse and complex executive branch function successfully within a centralized IT environment.

The goal of this document is to:

- Define services in terms that make sense to the customers
- Match the dollars, currently budgeted by the state agency for information technology with the services currently received from MN.IT Services
- Identify the processes by which agency business leadership can, with help from MN.IT Services, make business decisions and set priorities for information technology
- Clarify roles so that agencies know what IT delivers and who does what
- Quantify metrics and accountability so that agency business leadership knows that the documented expectations are being met.

To reinforce the nature of this Agreement as a planning tool and a covenant between two entities that co-exist under the jurisdiction of the executive branch and the leadership of the Governor of Minnesota, this Agreement is a document that requires neither a signature nor a “lock” on its content.

While the Agreement documents a set of expectations and warranties by which the individual agency customers can measure MN.IT’s service performance, it is also – more importantly - a vital planning tool for the agencies to set priorities and work with MN.IT Services in order to establish services and systems that have a high business value and meet the ever- changing program needs of the agency and its citizen customers.

For MN.IT Services, this document represents an opportunity to articulate and confirm its understanding of agency needs and expectations. It also serves as a baseline by which MN.IT can normalize and standardize roles, service levels, budgets, processes and procedures among its agency-based offices. It also allows the organization to identify centers of excellence, investment priorities, gaps and issues, and opportunities for leveraging resources and economies of scale.

In sum, this Agreement serves as the primary tool for an ongoing cooperative relationship that promises effective information technology management and enhanced government innovation to meet complex agency business needs in the decades ahead.

Substantiating Documentation

MN.IT Services intends to use five documents as the foundation for the direction of the State's IT program and the parameters of the Agency's goals and service management practices:

- This comprehensive Agreement focuses on the "nuts and bolts" of agency expectations and service accountability.
- The State of Minnesota Information and Telecommunications Systems and Services Master Plan that articulates the higher-level business goals and ambitions for technology at the State.
- The Agency Centralized IT Reference Model that sets the foundational direction for agency-based service delivery and customer relationships and facilitates MN.IT Services' ability to deliver consistent IT services and maintain accountability and responsiveness to all agencies, regardless of the diversity of business, resources and physical location.
- The Minnesota IT Governance Framework, that outlines the governance processes by which IT direction and priorities are set and how agencies participate and provide input.
- The MN.IT Services Tactical Plan, which details the goals and milestones of a multi-project effort to optimize IT services and maximize efficiencies in order to better service its customers.

Section 1: Service Agreement

MNsure Service Agreement

Introduction

The aim of this Agreement is to provide a basis for close co-operation between the Office of MN.IT Services (MN.IT) and MNsure (Agency), for support services to be provided by MN.IT to the Agency, thereby ensuring timely, cost effective and efficient support services are available to Agency end users.

The primary objective of this document is to define the service delivery items that will govern the relationship between MN.IT and the Agency. The SLA documents the required business facing information technology (IT) services that support the existing Agency business processes at the existing service levels. This SLA determines the IT service delivery performance baseline from which any desired future changes will be negotiated.

This SLA, and all appendices which are incorporated herein by reference, supersede in their entirety any previous agreements between the Office of MN.IT Services and the Agency 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. This SLA is intended to serve as a transitional agreement delineating the parties' responsibilities until superseded by future amendments.

For purposes of this SLA, "information technology" is defined as the acquisition, storage, communication, and processing of information by computers, telecommunications, applications and other software. This information includes, but is not limited to business data, voice, images, and video. IT provides businesses 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, all enterprise and agency-specific (unique) applications (business application software and related technical support services), system software, networks, databases, telecommunications, data centers, mainframes, servers, desktops and monitors/laptops/mobile computing devices, output devices such as printers, electronic mail, office systems, reporting, and other standard software tools, helpdesk, 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 of Service Level Agreements

- To create an environment that is conducive to a cooperative relationship between MN.IT and the Agency to ensure the effective support of end users who conduct state government business
- To document the responsibilities of all parties taking part in the Agreement
- To ensure that the Agency achieves the provision of a high quality of service for end users with the support of MN.IT
- To define the start of the Agreement and the process for reviewing and amending the SLA
- To define in detail the services to be delivered by MN.IT and the level of service and anticipated costs that can be expected by the Agency, thereby reducing the risk of misunderstandings
- To provide a common understanding of service requirements/capabilities and of the principles involved in the measurement of service levels/objectives
- To provide the parties to the SLA a single, easily referenced document that addresses the objectives as listed above

Agreeing Parties

The Office of MN.IT Services (MN.IT)

MNsure (Agency)

Agreement Schedule

Start Date: February 6, 2015

Review Process

This Agreement will be reviewed no less frequently than annually on a mutually agreed upon date, by the Agency and MN.IT. The review will include an evaluation of the services provided and service levels required by the Agency as of the date of the review. To the extent reasonably necessary to meet the business needs of the Agency, the parties to this SLA agree to use best efforts to amend the SLA to change and update the Agreement to reflect the Agency's business needs.

Contact Details

The following contacts are responsible for the monitoring and maintenance of this Agreement. Please refer to Section 2 for how to make operational requests.

	Name	Phone	Email address
Agency Primary Contact:	Scott Leitz	651/539-1320	scott.leitz@state.mn.us
MN.IT Services Contact:	Ann T Sessoms	651/431-2908	ann.sessoms@state.mn.us

Responsibilities

MN.IT and the Agency will establish a cooperative relationship to achieve efficiencies and improve the delivery of technology services in state government and to citizens, in which MN.IT will act as the IT service provider and the Agency will act as the customer.

In consideration of the mutual promises set forth in this SLA, MN.IT and the Agency agree to all terms in this SLA, including as follows:

In conjunction with state agencies and others stakeholders, MN.IT will establish and maintain a formal governance process (Minnesota IT Governance Framework) that includes agency business participation and incorporates agency input into overall IT strategy and direction.

All Agency-based IT-related employees are accountable to the Agency-based chief information officer (CIO) and, through the Agency-based CIO, report to the State CIO or designee. All Agency-based IT-related employees are MN.IT employees, but the Agency will continue to provide a portion of the support services, as agreed upon and as needed. (Hereinafter Agency-based IT-related employees are referred to as Agency-based MN.IT employees.)

MN.IT reserves and may exercise, during the term of the SLA, the right to assume the salary and other costs, provision of support services and administrative responsibility for Agency-based MN.IT employees for the purposes of complying with the IT Consolidation Act and improving Agency IT services, reassigned roles and/or service consolidation. It is anticipated that some of these changes will commence in fiscal year 2013.

MN.IT's oversight authority includes, but is not limited to, IT-related planning activities, budget management, purchasing, policy development, policy implementation, and direction of Agency-based MN.IT employees. MN.IT's oversight authority does not extend to the non-IT portions of the Agency's business operations.

Pursuant to Minnesota Statutes section 16E.016, MN.IT has the authority and is responsible for the provisioning, improvement, and development of all Agency IT systems and services as directed and delegated by MN.IT to the Agency-based CIO. In performing these duties, MN.IT will take into consideration all of the Agency's concerns and requests, as reasonably required to address the Agency's business needs.

All IT-related funds remain under the control of the Agency for accounting and administrative purposes, and MN.IT will direct and delegate authority for the management of those funds to the Agency-based CIO. All IT-related resources, regardless of funding source, constitute the Agency budget for IT (IT Budget). The Agency's total IT Budget includes, but is not limited to, budgets/funds for: Agency-based MN.IT employee salaries and fringe benefits; IT-related hardware, software, equipment, and asset maintenance; IT-related space rental, maintenance, and utilities; and IT-related professional internal and external services and all other IT-related contracts. The IT Budget includes, but is not limited to, the resources supporting the Agency IT-related activity or service components in all Agency divisions or units. The IT Budget will be considered to constitute the full and complete Agency budget for all IT activity at the Agency. The IT Budget does not include Agency resources that are outside the IT Budget.

MN.IT, through the Agency-based CIO and in consultation with the Agency, and the Agency chief financial officer (CFO), agrees to manage existing Agency-based IT resources consistent with this SLA. MN.IT intends to comply with all legal restrictions and requirements on those resources, if any.

MN.IT Services Roles and Responsibilities

MN.IT will exercise all authority and responsibilities in a manner that assures the best interests of the State and the Agency it serves while meeting the intent of the IT Consolidation Act as interpreted by the State CIO.

MN.IT is responsible for:

- Managing all IT strategic planning and establishing the State's IT direction in the form of policies, standards, guidelines and directives.
- Developing and determining delivery strategies for all executive branch state agency IT activity and services consistent with the Minnesota IT Governance Framework.
- Managing IT resource deployment at the executive branch level based on strategic planning, service delivery strategies, Agency and executive branch business needs and legal restrictions and requirements on IT resources and IT resource funding.
- Performing human resources services for the Agency-based MN.IT employees. MN.IT Human Resources (HR) has authority with regard to IT related employment including, but not limited to, transactions, classification, compensation, staffing, labor relations,

unemployment, workforce planning, recruitment, training & development, and safety &. MN.IT HR will work closely with the agency based HR offices on employment matters that were pending prior to this SLA.

- Delegating appropriate authority to the Agency-based CIO and providing direction and guidance to the Agency-based CIO in Agency IT business operations including, but not limited to, IT-related planning, budgets, purchasing, service strategy, policy development and implementation, and personnel management of Agency-based MN.IT employees.
- Determining responsibility, role, and compensation for the Agency-based CIO; creating a position description, completing performance appraisals of the Agency-based CIO and implementing performance-related measures including performance management, in consultation with the Agency.
- Providing guidance on the roles and responsibilities of MN.IT, the Agency-based CIO and the Agency related to the management and responses to data requests made under Minnesota Statutes chapter 13 for Agency data or information that resides on MN.IT-managed technology equipment. Agency data or information that resides on MN.IT-managed technology equipment is subject to Minnesota Statutes chapter 13 and MN.IT will comply accordingly.
- Promptly notify Agency, through the Agency-based CIO, of a known or suspected IT security breach of Agency's not public data. MN.IT will work with Agency to comply with notice and regulatory requirements under Minnesota Statutes chapter 13 and other applicable state and federal laws, rules and regulations. MN.IT and Agency-based CIO will work to identify the deficiency that led to the breach and to correct, mitigate and remediate the deficiency, which may require additional resources. Additional details regarding the requirements and coordination of IT security data breaches are included in the Enterprise Information Security Incident Management Standard (available on the MN.IT website).
- Working with Agency-based CIO and Agency regarding implementation of a MN.IT employee training program to satisfy applicable federal and state requirements for Agency data access and handling, if any. Additional details regarding the requirements and coordination of data training are included in the Enterprise Information Security Training and Awareness Standard (available on the MN.IT website).
- Implementing and maintaining appropriate IT internal controls for all IT-related business in accordance with MN.IT, Agency, and MMB policies, standards, and guidance. MN.IT is not responsible for maintaining internal controls for Agency non-IT related business.
- MN.IT, through the Agency-based CIO, intends to and will work in good faith with Agency to comply with all applicable state and federal laws, rules and regulations. MN.IT intends to and will work with Agency to comply with the additional Agency-specific legal and/or regulatory requirements located in Appendix A. If the Agency is not in compliance at the time of transition (July-August 2012) then additional resources may be required to bring Agency into compliance.

The Agency-based Chief Information Officer Roles and Responsibilities

The Agency-based CIO represents MN.IT at the Agency and has delegated oversight over all Agency-based MN.IT resources and employees. The Agency-based CIO has the authority and responsibility to:

- Manage the centralized reporting structure for all Agency-based MN.IT employees in consultation with the Agency and under the direction of MN.IT.
- Manage the Agency IT Budget, including the determination of service delivery strategies for IT services.
- Hire and manage Agency-based MN.IT employees, in coordination with human resources personnel, including, but not limited to, managing the work direction, selection, evaluation, reallocation, promotion, recognition, and coaching; administering disciplinary actions when necessary; and responding to any disputes or grievances filed by MN.IT employees.
- Manage and approve all IT purchasing consistent with Minnesota Statutes Chapter 16C and other applicable laws, and in consultation with the Agency.
- Represent the Agency's strategic IT direction, planning, business needs and priorities to MN.IT.
- Comply with and implement at the Agency all MN.IT IT policies, standards, guidelines, direction, strategies, and decisions.
- Comply with and implement at the Agency all Agency policies, standards, guidelines, direction, strategies, and decisions, unless in conflict with MN.IT IT policies, standards, guidelines, direction, strategies, and decisions.
- Report directly to and be held accountable by MN.IT for IT operational direction including, but not limited to, IT-related planning activities, budget management, purchasing, policy development, policy implementation and management of Agency-based MN.IT employees.
- Manage the oversight and authority for Agency IT-related activities - including, but not limited to, performance and functionality of Agency IT systems and applications - in a manner that supports statewide direction and policies established by MN.IT; enables appropriate technology, methodology, and industry best practices as directed by MN.IT; and advances the vision, mission, goals, and business needs of the Agency.
- Assist Agencies, as requested, with the prompt fulfillment of requests made pursuant to Minnesota Statutes chapter 13 for Agency data or information that resides on MN.IT-managed technology equipment. The responsibilities of MN.IT, the Agency-based CIO, and the Agency related to these requests are further delineated in MN.IT's data practices requests guidance document (issued Jan 3, 2012, revised April 3, 2012).
- Notify MN.IT of a known or suspected IT security breach of Agency's not public data, and promptly notify Agency of a known or suspected IT security breach of Agency's

not public data. Agency-based CIO will work with MN.IT and Agency to comply with notice and regulatory requirements under Minnesota Statutes chapter 13 and other applicable state and federal laws, rules and regulations. Agency-based CIO will work with MN.IT to identify the deficiency that led to the breach and to correct, mitigate and remediate the deficiency. Additional details regarding the requirements and coordination of IT security data breaches are included in the Enterprise Information Security Incident Management Standard (available on the MN.IT website).

- Consult and coordinate with MN.IT and the Agency regarding implementation of a MN.IT employee training program to satisfy applicable federal and state requirements for Agency data access and handling, if any. Additional details regarding the requirements and coordination of data training are included in the Enterprise Information Security Training and Awareness Standard (available on the MN.IT website).
- Work in good faith with MN.IT and Agency to comply with all applicable state and federal laws, rules and regulations. Additional Agency-specific legal or regulatory requirements may be located in Appendix A.

All Agency-based CIO decisions made and discretion exercised pertaining to this SLA are subject to the authority of MN.IT.

The Agency Roles and Responsibilities

In matters related to this SLA, the Agency is responsible for the following:

- Maintaining the Agency-based CIO in a role within the Agency that directly communicates with the Commissioner, Deputy Commissioner, or equivalent incumbent.
- Including the Agency-based CIO as a regular attendee of Agency executive team meetings to provide IT-related reports and ensure that the MN.IT IT strategy supports the business needs of the Agency.
- Communicating with the Agency-based CIO regarding all important Agency IT developments.
- Affording the Agency-based CIO with the authority appropriate to an Agency employee that will enable the Agency-based CIO to manage the IT Budget on the Agency's behalf in cooperation with Agency. This includes, but is not limited to, Agency IT purchasing authority.
- Determining and communicating new service requirements to the Agency-based CIO based on program needs, including, but not limited to, changes in service volumes and IT projects, identifying funds for new services, and initiating a change to this SLA and/or the IT Budget, as prescribed by the SLA and this Section.
- Providing input to the State CIO on performance appraisals and performance management for the Agency-based CIO.
- Continuing to perform all financial accounting services for the Agency's total IT

Budget, including, but not limited to, providing the Agency-based CIO with regular financial reporting sufficient to plan, manage and commit funding for Agency IT services, as well as fiscal operations and functions related to the Agency-based CIO and Agency-based MN.IT employees.

- Agency-based HR offices retain responsibility for any legal matters involving an Agency-based MN.IT employee initiated prior to this SLA, and will work closely with MN.IT HR.
- Continuing to perform a portion of the other administrative services, including responding to data requests under the Minnesota Government Data Practices Act (Minnesota Statutes chapter 13) and legislative functions, as needed and agreed upon by the parties to this SLA.
- As the "responsible authority" for Agency data or information, the Agency must respond to requests made pursuant to Minnesota Statutes chapter 13 for Agency data or information that resides on MN.IT-managed technology equipment. The responsibilities of MN.IT, the Agency-based CIO, and the Agency related to these requests are further delineated in MN.IT's data practices requests guidance document (issued Jan 3, 2012, revised April 3, 2012).
- Notifying Agency-based CIO of any suspected or known IT security breach of Agency's not public data. Agency will work with MN.IT to comply with notice and regulatory requirements under Minnesota Statutes chapter 13 and other applicable state and federal laws, rules and regulations. Agency is responsible for providing any required notifications under Minnesota Statutes section 13.055 and other applicable state and federal laws, rules and regulations. Additional details regarding the requirements and coordination of IT security data breaches are included in the Enterprise Information Security Incident Management Standard (available on the MN.IT website).
- Working with Agency-based CIO and MN.IT regarding implementation of a MN.IT employee training program to satisfy applicable federal and state requirements for Agency data access and handling, if any. Additional details regarding the requirements and coordination of data training are included in the Enterprise Information Security Training and Awareness Standard (available on the MN.IT website).
- Working in good faith with MN.IT and the Agency-based CIO to comply with all applicable state and federal laws, rules and regulations. Additional Agency-specific legal or regulatory requirements may be located in Appendix A. If the Agency is not in compliance at the time of transition (July-August 2012) then additional resources may be required to bring the Agency into compliance.

Acceptance, Amendments, and Termination

MN.IT's provision of services under this SLA and the Agency's use of those services constitutes acceptance by both parties of all terms in this SLA.

Any amendment to this Section 1, Appendix A , or Appendix B, or termination of this SLA, must be in writing and will not be effective until it has been approved by the State CIO and the Agency Primary Contact identified above. Either party may request an amendment to this Section in writing, with full documentation of purpose and justification.

To make a change to the IT Budget, the Agency's CFO must provide notice, and a reason for the change, to MN.IT's CFO and the Agency-based CIO, and MN.IT's CFO will consult with MMB. A change to the IT Budget may also require a change to the SLA.

Except for Section 1 and Appendices A and B, any other changes to the SLA, including service levels, must be in writing and will not be effective until approved by the State CIO, or designee, and the Agency Primary Contact identified above, or designee. The State CIO, or designee, and the Agency Primary Contact identified above, or designee, may agree to establish a more efficient process to change the SLA (other than Section 1 and Appendices A and B) but all changes must be in writing. A change in service levels may also require a change to the IT Budget, which must follow the process in the preceding paragraph.

Dispute Resolution

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 communications and engage 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 Primary Contact and the State's CIO will meet to determine further action.

Liability

Each party shall be responsible for claims, losses, damages and expenses which are proximately caused by the wrongful or negligent acts or omissions, including lack of funding, of that party or its agents, employees or representatives acting within the scope of their duties. 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 or be construed to create a basis for any claim or suit when none would otherwise exist. This provision shall survive the termination of this Agreement.

Additional Provisions

The terms of this SLA are not meant 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 Agreement shall be governed by the laws of the State of Minnesota. Venue for all legal proceedings arising out of this Agreement, or breach thereof, shall be in the state or federal court with competent jurisdiction in Ramsey County, Minnesota.

Assignment

Neither MN.IT 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 MN.IT's ability to use third party contractors or products to meet its obligations under this SLA.

Section 2: Service Operations

Service Operations

Customer Service

Customer Relations

Agency-based MN.IT Chief Information Officer (CIO)

The Agency-based CIO has been and will continue to be an integral part of the Agency management team and the primary agency partner for the development of IT plans and the manager of IT solutions that meet the Agency's business needs. Working with Agency business leaders, MN.IT's Agency-based CIO will plan, design, create and maintain IT solutions and work with the Agency to meet service levels, budgets and priorities.

Specifically, the MN.IT Agency-based CIO:

- Leads technology planning, needs assessment, design, and procurement of IT for the Agency
- Partners with Agency business leaders to design create and maintain applications to meet business requirements
- Manages delivery and ongoing operational support of IT at the Agency level
- Provides and reviews with Agency leadership all service level reporting.

MN.IT Services Account Team

Each MN.IT customer also has a designated Account Team for those services that are provided centrally by MN.IT Services. The Account Team is comprised of a primary and backup Account Manager to work with the Agency-based CIO on provisioning and sourcing the central services the Agency needs.

Specifically, the Account Manager:

- Provides consultation; needs assessment; analysis and design of cost-effective centrally provided solutions to meet business needs
- Leverages the full resources of MN.IT's technical expertise to deliver centrally provided solutions to Agency business needs and/or to source them from private partners
- Develops proposals and service agreements for utility and other MN.IT centrally provided services
- Provides service level reporting and reviews, jointly with the Agency-based CIO, on utility and other MN.IT centrally provided services.

The Agency-based CIO and Account Manager are integral parts of the MN.IT team working to bring the Agency the best technology to meet the Agency's needs at the best price performance possible.

Service Level Reporting

Reporting

Recurring service performance reports will be run against the service level targets defined in Section 4. This performance report will be in the form of a monthly IT dashboard with the following attributes:

- Availability
- Capacity
- Service Support
- Recoverability

Reviews

Service reviews will be conducted on a quarterly basis and facilitated by the Agency-based CIO through the service level management process.

Requesting Support for MN.IT Services

While every Agency-based office currently manages individual processes and procedures for the support of Agency-based IT services, MN.IT Services, in this document, sets forth standards for service management based on the standard for current centrally delivered services. These standards apply to all service desks, regardless of location, unless otherwise noted.

Following the standards in this section, are the processes and exceptions that are currently in effect at the Agency.

Agency-based CIOs, as a group, are working to define common service management processes that will bring all MN.IT services into alignment with enterprise-wide standards in the future. This SLA will be amended by the Agency-based CIO as changes are made to the specific procedures at the Agency.

MN.IT Service Desk

The MN.IT Service Desk acts as the central point of contact for all IT services. It is the focal point for reporting all service incidents and for all service requests. The MN.IT Service Desk is a skilled, 24x7 on-site operation that performs the first line support for all IT services, fulfilling a large percentage of incidents and requests without escalation.

Definitions

Incident: An incident is any event which is not part of the standard operation of service and which causes, or may cause, an interruption or a reduction in the quality of that IT service.

Service Request: A user request for support, delivery, information, advice, documentation, or a standard change. Service requests are not service disruptions.

Service Desk Activity

Ownership, monitoring, and tracking of all incidents and requests: 100**%** logging of incidents/ requests; request managed throughout their lifecycle.

Customer-facing first level support for all services: Response to all submitted incidents & requests through incoming calls, email, online and system monitoring alerts in a prompt & efficient manner; provision of customer status.

Escalation: Intensify the response to the incident or request; Coordinate handoff to second-line or third-party support groups, if necessary.

Communications: Communication of planned and unplanned service outages.

Critical Success Factors

The purpose for and criteria for measuring the success of the Service Desk include:

- **Maintaining IT service quality** –as documented in individual Service Level Agreements
- **Maintaining customer satisfaction** – per customer survey metrics
- **Resolving incidents within established service times** – See Service Level Objectives in table below
- **Fulfilling requests within established service times** – See Service Level Objectives in table below

Prioritization

All incidents and service requests will be assessed and assigned a priority based on two criteria**: urgency** and **impact**. Priority drives the incident resolution and request fulfillment process and associated procedures.

Priority Level	Definition	Incident Management and Request Fulfillment Service Objectives
Critical-1	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.	2 Hours (24x7)
High-2	Any incident that impacts a significant number of users, a major agency application or service, but has redundancy, or an alternate path or bypass.	8 Hours (24x7)
Medium-3	Any incident that impacts a limited number of users with a resource or service down or degraded.	2 Business Days*
Low-4	Any incident that impacts a small number or a single user in which a resource or non-critical service is down or degraded and a deferred fix or maintenance is acceptable.	5 Business Days*

*Business Day = Monday – Friday 8:00 AM – 5:00 PM

Critical-1 Procedures

The MN.IT Service Desk follows Critical-1 escalation and notification procedures 24 hours a day, seven days a week, 365 days a year.

A master incident ticket serves as the source document throughout the event and this ticket number is referenced in all updates regarding the incident.

Stages	Activity	Agency Communications	Notification Objectives
Critical-1 Incident is identified	Agency is notified that a Critical-1 incident is in progress	Email sent to Critical-1 distribution list Service Desk ACD (Automated Call Distributor) is updated	Within 20 minutes of Critical incident being identified

During a Critical-1 Incident	The Service Desk updates Agency regularly while the Critical-1 incident is occurring	Email to the Critical-1 distribution list Service Desk ACD message updated	Every hour, on the hour or as pertinent information becomes available
Critical-1 Incident is resolved	Agency is notified of resolution	Email to the Critical-1 distribution list Service Desk ACD message updated.	Within 10 minutes of resolution
After-Action Analysis and Agency follow-up	Problem Management holds an after-action meeting within 3 business days to review the root cause and define process improvements that can mitigate or prevent future occurrences	A Root Cause Analysis (RCA) report is emailed to the Critical-1 distribution list.	Within 2 business days of the after-action meeting.

MN.IT Central Service Desk Contact Information

(See following pages for information on the Agency-based MN.IT Service Desk)

Business Hours	24 x 7 x 365
Contact Name	MN.IT Service Desk
Phone Number	651-297-1111
Email Address	Service.Desk@state.mn.us
Web Site and Service Catalog	www.MN.gov/oet

Scheduled Maintenance and Changes for MN.IT Services

To ensure the stability, service levels, and availability of services, MN.IT Services uses *change windows* to implement planned changes and maintenance that carry a risk of or are known to impact a service. Requests for maintenance or changes are planned, reviewed, authorized, scheduled and controlled to occur during these windows in order to ensure that they are successful and fully completed within the scheduled change window.

Each request for maintenance or change is:

- **Planned** to ensure prior testing, where possible, proper time estimates, successful change validation testing, and allowance for time to back out the change if problems cannot be resolved.

- **Reviewed** to ensure the plan is appropriate, complete and doesn't conflict with other changes.
- **Authorized** after having had proper levels of approvals, risk assessments, and plans.
- **Scheduled** to avoid conflicts with other changes, mitigate risks and minimize disruption to business.
- **Controlled** to ensure proper process, resources, and execution.
- **Logged/tracked** to ensure that changes are documented in order to facilitate review and control.

Following these procedures ensures the highest success rate with appropriate risk, and minimizes the potential for any interruption in service. In the event the authorized work cannot be successfully completed in the scheduled window, it will be backed out, the service / technology infrastructure will be returned to the previous baseline, the cause for failure will be determined, an implementation plan will be updated, and the change will be authorized for a subsequent window.

Scheduled Maintenance / Change Windows

MN.IT will provide Agency a 5-day advance notice of Scheduled Maintenance. All prescheduled systems maintenance, unless otherwise agreed upon in advance by Service Operations, shall be during the time specified in the scheduled maintenance/change window as follows:

The service unavailability for scheduled maintenance windows is excluded from uptime (availability) calculations. The maintenance is performed during the time specified in the scheduled maintenance/change window.

Emergency Maintenance and Changes

Emergency changes are typically to resolve an ongoing service outage or degradation or address an emerging security vulnerability, in which case the risks and potential business impact are so high that it is not prudent to wait for the next regularly scheduled change window.

Under certain unforeseen circumstances, MN.IT may need to perform emergency maintenance or changes, such as security patch installation or hardware replacement. If MN.IT is unable to provide customers with advanced notice in cases of emergency maintenance, MN.IT will provide after-the-fact follow-up for the event.

MNsure Service Operations Details

MN.IT @ MNsure Service Desk

The MN.IT@ MNsure Service Desk has the following exceptions to the standards identified in Section 2: Service Operations.

General Information

Contact Information

Service Desk Name	ITS Help Desk
Business Hours	7:30-4:00
Contact Name	Kelle DeCosta
Phone Number	651/431-2224
Email Address	kelle.decosta@state.mn.us
Web Site and Service Catalog	http://workplace/fmo/gateway/Pages/ServiceCatalog.aspx

Prioritization

MN.IT@ MNsure Service Desk uses the following prioritization criteria:

Priority Level	Definition	Incident Management and Request Fulfillment Service Level Objectives
Stop work	An outage of MNsure enterprise wide services affects all users at a main campus, is likely to cause significant financial loss or critical data loss or seriously impairs regular ongoing work of MNsure as it relates to customers and business partners.	N/A
High	• Has an impact on clients or users and may cause financial or data los• Impairs non-routine work of MNsure as it relates to its customers & businesses, • No feasible workaround	N/A
Medium	• Has a limited or confinable impact on clients or users, • Minimal work impairment, • Reasonable workaround is available	N/A
Low	• Insignificant impact on clients or user, • Known reliable workaround is available	N/A

Critical-1 Procedures

MN.IT@ MNsure Service Desk uses the following Critical-1 Procedures:

Stages	Activity	Agency Communications	Notification Objectives
Critical-1 Incident is identified	Customers are notified of the outage/incident.	Subscribers to DHS ITS Notifications are notified of the outage/incident. ACD is updated	Initial communication within 15 minutes
During a Critical-1 Incident	The Help Desk updates IT notification regularly	Subscribers to DHS ITS Notifications are notified of the outage/incident. ACD is updated	Every hour as pertinent information becomes available.
Critical-1 Incident is resolved	Customers are notifified of resolution	Subscribers to DHS ITS Notifications are notified of the outage/incident. ACD is updated	As soon as resolution is verified
After-Action Analysis and Agency follow-up	A root caluse template is completed	N/A	N/A

Scheduled Maintenance / Change Windows

All prescheduled systems maintenance, unless otherwise agreed upon in advance by Service Operations, shall be during the time specified in the scheduled maintenance/change window as follows:

Monday thru Friday: [redacted]

Saturday: [redacted]

Sunday:

The service unavailability for scheduled maintenance windows is excluded from uptime (availability) calculations. The maintenance is performed during the time specified in the scheduled maintenance/change window.

Section 3: Standard IT Services

Standard IT Services

Introduction

MN.IT Services provides a wide range of technology solutions to agencies. These solutions can be grouped into four broad categories:

1. Standard IT Services
   Information technology solutions that facilitate day-to-day agency business operations. Examples include email, web sites, and telephone service. ***These services are listed in this section.***

2. Agency Applications
   Information technology solutions and Agency business applications that support Agency specific business requirements and related Agency business programs. These services are listed in Section 4.

3. Projects and Initiatives
   Services that deliver a specific outcome. These services are listed in Section 5.

4. Enabling IT Services
   IT solutions that enable the delivery of Standard IT Services and Business Services. Examples include local area networks, firewalls, and help desk services. These services are listed in Appendix D.

Standard IT Services

This section provides an overview of each **Standard IT Service** area and sets specific expectations regarding the performance parameters, delivery, and support of each service. The following Standard IT Services are described in detail on the following pages:

- **Connectivity and Mobility** - wireless access within state locations, virtual private network (VPN) access to state networks, and cellular service plans and devices.
- **Enterprise Unified Communications and Collaboration** - email accounts, email archiving, BlackBerry, ActiveSync, SharePoint, instant messaging, audio/video/net conferencing.
- **Facility Services** - audio-visual equipment and design services for conference rooms, training facilities, and laboratory areas.
- **•Minnesota Geospatial Information Office (MnGeo)** – geospatial coordination services, geospatial professional services, geospatial commons, geospatial infrastructure hosting

- **Security Services** – information security program management, identity and access management, auditing, password policies, forensics, incident management, security training and awareness. All security enabling services are embedded in business services as mandated by state security policies, standards and compliance.
- **Voice Services** - "classic" and voice over IP (VOIP) telephones, long distance, toll free numbers, calling cards, and other telephone-related services.
- **Web Management** - web server management, content delivery and migration, user interface design, information architecture, accessibility, Minnesota Geospatial Information Office (MnGeo) and search.
- **Workstation Management** - operating systems, hardware, software, accessories, peripherals, and security services related to desktop and laptop computers.

Support Hours and Service Availability

MN.IT Services' definition of service levels are designed to give agencies clear expectations for the quality of the services MN.IT provides. The following service documentation outlines the standard service levels for each MN.IT Standard Service, with exceptions noted for any anomalies at the individual agency level. These anomalies will be based on available resources and/or particular Agency business needs that have been identified by the Agency. The documented service levels and exceptions as described in this section reflect the "as is" level of service for Standard IT Services.

The support hours and level of service availability associated with each service are typically indicators of how critical the service is to agencies. In addition, the complexity and configuration of specific Standard IT Services will vary with each implementation. In most cases, the cost of a service is directly related to the level of service availability and reflects the resources necessary to achieve the desired level of service. Delivering a high level of support and availability requires that all resources associated with the service are available at equal levels. For example, a web hosting service depends on many factors including staffing hours, electrical power, networking, hardware, and software. If any one of these items is only available 99% of the time, then the overall service availability cannot exceed 99%. Different service availability levels can be described as follows:

- 99.9% - Maximum of 8 hours, 45 minutes of downtime per year. This level requires 24 x 7 staffing, "High Availability" (HA) system design, and redundant components.
- 99.5% - Maximum of 43 hours, 48 minutes of downtime per year. This level requires having staff "on call," spare parts, and/or maintenance contracts for parts delivery.
- 99.0% - Maximum of 87 hours 36 minutes of downtime per year. This level requires having staff "on call," well-defined system recovery procedures, and business hour staffing.

- Measuring a service availability level is very different from measuring reliability. A particular piece of equipment may operate 99.9% of the time - until it fails. If it takes 48 hours to implement a replacement when it fails, the service availability metric cannot exceed 99.5%.

In some cases, MN.IT Services contracts with external vendors to deliver services. The service metrics and availability for the contracted services reflect the reported and/or measured capabilities provided by the vendor.

In all cases, MN.IT staff provides support for contracted Standard IT Services. Agencies can call the MN.IT Service Desk 24 hours a day, seven days a week. The support hours for individual Standard IT Services may vary (and are listed in the following sections).

Depending on the stated service availability level, MN.IT staff may record the service request, but the information presented for each of these service areas sets a baseline level of expectations for service delivery.

When individual MN.IT services are mapped to specific Agency business requirements and Agency capabilities, the service metrics and key deliverables may be modified.

Connectivity and Mobility

Service Description Overview

MN.IT's Connectivity and Mobility services consist of 1) wireless access; 2) VPN remote access; and 3) cellular service plans and devices. This section provides a high-level description of these services.

- Wireless access: Allows laptops, tablets and other wireless capable devices to access MN.IT-managed wireless networks operating within State locations. This service can provide connections that are temporary ("guest" access for visitors while on-site) or can be subscribed for regular wireless network access. Guest wireless is configured for public internet access. Subscribed regular wireless access can be public internet access or connected to an internal (non-public) secure network.
- VPN Remote Access: A virtual private network (VPN) is a network that uses an internet based connection, to provide remote end users with secure access to their organization's network. A VPN user typically experiences the central network in a manner that is identical to being connected directly to the central network (e.g., access to files share and printers).
- Cellular Service Plans and Devices: MN.IT Services provide a number of cellular-based services to end users. Mobile devices range in size and weight and come in a number of form factors including cell phones, smart phones, tablets and pagers. Also included in this category are mobile "hotspots" which create a small area of Wi-Fi coverage off a cellular network connection, thus allowing nearby Wi-Fi devices to connect to the internet.

Service Metrics

Support Hours

- Wireless Access: normal business hours
- VPN Remote Access: 24 x 7 x 365
- Cellular Service Plans and Devices: normal business hours

Service Availability

Wireless Access

Service availability for Wireless Access is 99.9% and excludes time to perform routine or scheduled maintenance. Wireless Access service availability is calculated as follows:

$$\frac{\text{[Applicable days in calendar month x 24 x 60] Minus [Minutes of outage in calendar month]}}{\text{Applicable days in calendar month x 24 x 60}} \times 100$$

Scheduled downtime means those times where MN.IT Services notifies agencies of periods of Downtime for Scheduled Maintenance at least five days prior to the commencement of such Downtime. There will be no more than fifteen hours of Scheduled Downtime for Wireless Access per calendar year, and no more than two hours per month. Scheduled Downtime is not considered Downtime for purposes of this SLA, and will not be counted towards any Downtime Periods.

Downtime period is a period of ten consecutive minutes of Downtime. Intermittent Downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

Scheduled Downtime will be announced every month and be available to agencies. If a Scheduled Downtime conflicts with other activities/operations of an Agency, the Agency can request an alternate date for the Scheduled Downtime thru the MN.IT Service Desk. MN.IT Services will work with agencies to find a date that balances the needs/priorities of all.

VPN Remote Access

Service availability for Virtual Private Network (VPN) remote access is 99.9% and excludes time to perform scheduled maintenance. VPN remote access service availability is calculated as follows:

$$\frac{[\text{Applicable days in calendar month} \times 24 \times 60] \text{ Minus } [\text{Minutes of outage in calendar month}]}{\text{Applicable days in calendar month} \times 24 \times 60} \times 100$$

Scheduled Downtime means those times where MN.IT Services notifies agencies of periods of Downtime for Scheduled Maintenance at least five days prior to the commencement of such Downtime. There will be no more than fifteen hours of Scheduled Downtime for VPN per calendar year, and no more than two hours per month. Scheduled Downtime is not considered Downtime for purposes of this SLA, and will not be counted towards any Downtime Periods.

Downtime Period is a period of ten consecutive minutes of Downtime. Intermittent Downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

Scheduled Downtime will be announced every month and be available to agencies. If a Scheduled Downtime conflicts with other activities/operations of an agency, the agency can request an alternate date for the Scheduled Downtime thru the MN.IT Service Desk. MN.IT Services will work with agencies to find a date that balances the needs/priorities of all.

Incident Response Levels

The incident response levels associated with Connectivity and Mobility services match those identified in the Service Desk “Incident Management Quick Reference.” The following table lists examples of service incidents and the priority levels associated with them.

Table 1: Incident Response Levels for Connectivity and Mobility

Level	Example
Priority 4: Low	• Wireless Access – implement wireless access in a new location • VPN Remote Access – software installation and/or token replacement • Cellular Service Plans and devices – new device order
Priority 3: Medium	• Wireless Access – wireless access for an individual user is non-functional • VPN Remote Access – VPN access for an individual user is non-functional • Cellular Service Plans and devices – replacement device order
Priority 2: High	• Wireless Access – access for a group of users is non-functional • VPN Remote Access – VPN service is non-functional for multiple users • Cellular Service Plans and devices – localized service outage
Priority 1: Critical	• Wireless Access - access for a large group of users is non-functional • VPN Remote Access – VPN service is non-functional for all users • Cellular Service Plans and devices – widespread service outage

Service Level Objectives

The table below contain the Service Level Objectives for services within Connectivity and Mobility.

Table 2: Service Level Objectives for Wireless Access

Metric	Definition	Threshold
Service Availability	Measures the wireless infrastructure service availability	99.9% availability* *not including Downtime for scheduled maintenance
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Response	Measures the speed of request resolution by MN.IT Services	30 minutes for “guest” access; 2 business days for all other requests

Table 3: Service Level Objectives for VPN Remote Access

Metric	Definition	Threshold
Service Availability	Measures the VPN Remote Access service availability	99.9% availability* *not including Downtime for scheduled maintenance
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Response	Measures the speed of request resolution by MN.IT Services	2 business days

Table 4: Service Level Objectives for Cellular Service Plans and Devices

Metric	Definition	Threshold
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Response	Measures the speed of request resolution by MN.IT Services	5 to 7 business days after Purchase Order (PO) creation

Reporting

Reports for Connectivity and Mobility services are created monthly and made available to agencies. Specific reporting deliverables are listed below:

Wireless Access

- **Service Availability (monthly):** Percent of service availability for the month
- **Service Availability (12-month average):** Average percent of service availability for the prior 12 months

VPN Remote Access

- **Service Availability (monthly):** Percent of service availability for the month
- **Service Availability (12-month average):** Average percent of service availability for the prior 12 months

Cellular Service Plans and Devices

- **Number** of devices **(monthly):** Number of cellular devices within the business

Enterprise Unified Communications and Collaboration

Service Description Overview

Enterprise Unified Communication and Collaboration (EUCC) services delivered by MN.IT Services contain four distinct service offerings:

- EUCC Email
- EUCC SharePoint (Web Collaboration)
- EUCC Instant Messaging
- Audio, Video and Net Conferencing

A high-level description of these services is included here.

EUCC Email

- Email Service: EUCC Email is a single Enterprise Email and calendaring system that integrates existing state directories to preserve a single sign-on authentication. The EUCC Email service provides a “Standard” mailbox storage size of 5 Gigabytes (GB) per user.
- BlackBerry Gateway: Support the interface to the email system which utilizes the BlackBerry gateway.
- Email Storage: Agencies can increase the standard mailbox storage size to 25 GB on a per-user basis, by changing the mailbox type from “Standard” to “Executive” (thus providing 20 GB of additional storage to the standard mailbox). Changing the mailbox type will result in additional storage fees. The user is responsible for managing his/her mailbox within the assigned mailbox storage maximum.
- Email Archiving: Email archiving is the management and long-term storage of important emails - including attachments - independent from an individual user’s mailbox. Depending on specific business and legal requirements for data retention, each Agency may choose to utilize the archiving service differently.

EUCC SharePoint

- Collaboration: EUCC SharePoint provides a flexible, web-based solution that includes tools and services to help users manage information, collaborate effectively, share documents, search for information, define workflow process, and develop custom applications.
- Integration: The EUCC SharePoint environment leverages the state’s infrastructure of co-located Domain Controllers to provide all users with integrated single sign-on, cross-organization information sharing, and full Microsoft Office connectivity.
- Administration: Agencies receive full Administrator control of their Site Collections.

- Secure Access: SharePoint web applications deliver content via 128-bit SSL encryption.
- “Connect” site collections are intended for cross-organizational sites composed of users from multiple organizations.
- “Inside” site collections are intended for intranet sites governed by a single organization.
- “People” sites provide My Sites functionality for all SharePoint users.
- Site Collections: The EUCC SharePoint service can provide both “Standard” 100 GB and “Extra Large” 400 GB site collections on the “Inside” and “Connect” web applications. Personal sites (My Sites) are supported with a storage limit up to 7 GB/user.
- Storage: Agencies are allocated 500 MB per user, aggregated across the Agency’s organization. Additional storage is available for a fee.

EUCC Instant Messaging

- Instant Messaging: Instant Messaging (IM) is a growing communications method for short, "bursty" conversations which are too time-consuming for email. Instant Messaging enables users within organizations and across organizations to communicate in a faster, more real-time conversation, thus enhancing efficiency. EUCC IM also has the ability to facilitate person-to-person or group audio, video and net conferences. These conference functions use the audio components of PCs and can be enhanced with USB video cameras and audio headsets. As an added benefit, instant messaging is tightly integrated with EUCC Email which allows users to determine the "presence" of other users. Presence indicates a person's availability to establish communication (away, available, busy, in a meeting, etc.)
- Instant Messaging Federation: Instant messaging federation enables separate Office Communications Server installations to communicate with each other. All federated communications are encrypted between the IM systems using access proxy servers. MN.IT Services has no control over encryption after messages are passed to the federated partner’s network.

Audio, Video and Net Conferencing

- Audio Conferencing: An audio conference account with MN.IT provides agencies with access to a suite of conferencing solutions. This service includes options that allow the participants to dial-in to a designated central number or be a part of Operator-Assisted calls. Audio conferences can be reservation-less (agencies are given a permanent conference code that can be used at any time) or reserved; reservation-less conferencing is the typical user tool, whereas reserved conferences are generally for large and/or high-profile events. Toll, toll-free, dial-in and dial-out calling options are also available, as are recording, transcription and other advanced services.
- Video Conferencing: Video conferencing services are supported by MN.IT at several operational levels:

  - Video Conference Room Support Services: MN.IT staff work collaboratively with the Agency to support their conference planning, connection set-up and participant training (to provide basic operational support during calls such as positioning cameras, or muting microphones).
  - Desktop Video Client Accounts can be installed on PCs and some mobile devices and registered to MN.IT infrastructure to enable person to person calls, person to video conference room calls, or group (multi-site) calls.
  - Video Conference Network Services help agencies deploy and operate rooms or PC clients with a suite of video conferencing network services including Quality of Service (QoS) network management, statewide dialing plan, conference scheduling systems, bridging, event recording, and streaming options.

- Net Conferencing: A net conference account with MN.IT provides agencies with access to a set of conferencing solutions that support a wide variety of use cases, event configurations and needs. Net conferencing accounts are available in two ways: by subscription, or by per-minute usage. The per-minute usage capability is part of the contracted audio conferencing service.
  - Subscription services provide access to specialized net conferencing environments to support meetings, training, large events, and technical support needs, with presenter and participant options tailored to unique requirements of the different situations.
  - Per-minute usage services are used only for the meeting tools, which tend to be more than adequate for the typical user who does not run or stage training, large events or do technical support for end-users.

  During a net conference of any type, audio usage charges may also apply if using the integrated audio services available with the net conference account. Recording and editing functions are also available.

  Note: EUCC Instant Messaging also provides net conferencing services. See EUCC Instant Messaging within this document for additional information.

Service Metrics

Support Hours

Support hours for EUCC Email, EUCC SharePoint and EUCC Instant Messaging services are provided 24 x 7 x 365.

Support hours for Audio, Video and Net Conferencing services are provided during normal business hours.

Service Availability

Service availability for all Enterprise Unified Communication and Collaboration services is 99.9%. This excludes time to perform routine or scheduled maintenance. EUCC service availability is calculated as follows:

$$\frac{[\text{Applicable days in calendar month} \times 24 \times 60] \text{ minus } [\text{Minutes of outage in calendar month}]}{\text{Applicable days in calendar month} \times 24 \times 60} \times 100$$

Scheduled downtime means those times where MN.IT Services notifies agencies of periods of Downtime for Scheduled Maintenance at least five days prior to the commencement of such Downtime. There will be no more than fifteen hours of Scheduled Downtime per calendar year, and no more than two hours per month. Scheduled Downtime is not considered Downtime for purposes of this SLA, and will not be counted towards any Downtime Periods.

Downtime period is a period of ten consecutive minutes of Downtime. Intermittent Downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

Scheduled Downtime will be announced every month and be available to agencies. If a Scheduled Downtime conflicts with other activities/operations of an agency, the Agency can request an alternate date for the Scheduled Downtime thru the Service Desk. MN.IT services will work with agencies to find a date that balances the needs/priorities of all.

Service availability is focused on the following elements within each EUCC service area.

- EUCC Email: Service availability includes Outlook Web Application (OWA), the full Outlook Client, Microsoft ActiveSync service and BlackBerry services.
- EUCC SharePoint: Service availability includes one or more SharePoint site collections. Agencies select their own site collection administrators who in turn define and delegate the specific features and permissions available to their users. Most SharePoint Standard and Enterprise features are available for use within site collections. Some EUCC SharePoint features and functionality must be enabled through a change request process managed by MN.IT Services. Details about individual EUCC SharePoint features are contained in the “EUCC SharePoint Service Description” document.
- EUCC Instant Messaging: Service availability includes Communicator Web Access, the Microsoft Lync Instant Messaging client.
- Audio, Video and Net Conferencing: Service availability includes audio conferencing, video conference network infrastructure and net conferencing.

Incident Response Levels

The incident response levels associated with Enterprise Unified Communication and Collaboration services match those identified in the Service Desk “Incident Management Quick

Reference. The following table lists examples of service incidents and the priority levels associated with them.

Table 5: Incident Response Levels for Enterprise Unified Communication and Collaboration

Level	Example
Priority 4: Low	• EUCC Email – Delegation assignment; Free/busy not updating • EUCC SharePoint – Alert notification not working for individual users • EUCC Instant Messaging – audio and video hardware issue for individual users • Audio, Video and Net Conferencing – software incompatibility on individual user workstation
Priority 3: Medium	• EUCC Email – Mobile device not sending/receiving messages; user cannot login • EUCC SharePoint – Individual user cannot access SharePoint site. • EUCC Instant Messaging – IM, desktop sharing, presence or login not working for individual users • Audio, Video and Net Conferencing – Cannot start audio, video, or net conference
Priority 2: High	• EUCC Email – access or functionality for a group of users is non-functional • EUCC SharePoint – access or functionality for a group of users is non-functional • EUCC Instant Messaging – access or functionality for a group of users is non-functional • Audio, Video and Net Conferencing – access or functionality for a group of users is non-functional
Priority 1: Critical	• EUCC Email – access for a large group of users is non-functional • EUCC SharePoint – access for a large group of users is non-functional • EUCC Instant Messaging – access for a large group of users is non-functional • Audio, Video and Net Conferencing – access for a large group of users is non-functional

Service Level Objectives

The tables below contain the Service Level Objectives for the specified EUCC services.

Table 6: Service Level Objectives for EUCC Email Services

Metric	Definition	Threshold
Service Availability	Measures service availability. Combined with other metrics, gives an end-to-end view of EUCC as a managed service	99.9% availability** not including Downtime for scheduled maintenance

Metric	Definition	Threshold
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by the MN.IT Service Desk	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Response	Measures the speed of request resolution by the MN.IT Service Desk	All requests will be entered as "Medium" with 2 business days for resolution, unless specifically listed. Requests can be escalated on a case-by-case basis.
BlackBerry device - disable/wipe requests	In the event a BlackBerry device is lost or stolen, it can be disabled and remotely "wiped".	Escalated cases will be done within 1 hour of request; all others are completed in 1 business day.
Mail Flow	Measures the amount of time it takes to deliver a synthetically generated message	90% of messages received in less than 90 seconds

Table 7: Service Level Objectives for EUCC SharePoint Services

Metric	Definition	Threshold
Service Availability	Measures service availability. Combined with other metrics, gives an end-to-end view of EUCC as a managed service	99.9% availability* *not including Downtime for scheduled maintenance
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by the MN.IT Service Desk	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Response	Measures the speed of request resolution by the MN.IT Service Desk	All requests will be entered as "Medium" with 2 business days for resolution, unless specifically listed. Requests can be escalated on a case-by-case basis.

Metric	Definition	Threshold
SharePoint Site Access request	Determined by automated monitoring that attempts to render SharePoint sites every minute.	Customers have continuous access to all SharePoint sites for which they have appropriate permissions. Does not include scheduled downtime within pre-established maintenance windows

Table 8: Service Level Objectives for EUCC Instant Messaging Services

Metric	Definition	Threshold
Service Availability	Measures service availability. Combined with other metrics, gives an end-to-end view of EUCC as a managed service	99.9% availability** not including Downtime for scheduled maintenance
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by the MN.IT Service Desk	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Response	Measures the speed of request resolution by the MN.IT Service Desk	All requests will be entered as "Medium" with 2 business days for resolution, unless specifically listed. Requests can be escalated on a case-by-case basis.

Table 9: Service Level Objectives for Audio, Video and Net Conferencing Services

Metric	Definition	Threshold
Service Availability	Measures service availability.	99.9% availability* *not including Downtime for scheduled maintenance
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by the MN.IT Service Desk	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Response	Measures the speed of request resolution by the MN.IT Service Desk	All requests will be entered as "Medium" with 2 business days for resolution, unless specifically listed. Requests can be escalated on a case by case basis.

Reporting

Reports for EUCC services are created monthly and made available to agencies. Specific reporting deliverables are listed below:

EUCC Email

- **Service Availability (monthly):** Percent of service availability for the month.
- **Service Availability (12-month average):** Average percent of service availability for the prior 12 months.
- **Percentage of Spam and Virus detected:** Percent of email from the internet which are rejected because they contained spam or a virus.
- **Number of Mailboxes:** Total number of mailboxes in EUCC Email.
- **Number of BlackBerry devices:** Total number of BlackBerry devices connecting to EUCC Email.
- **Number of ActiveSync devices:** Total number of ActiveSync devices connecting to EUCC Email.
- **Email Volume (total):** Total number of emails received from the internet.
- **Email Volume (spam/virus rejected):** Total number of emails rejected from the internet because they contained spam or a virus.

EUCC SharePoint

- **Service Availability (monthly):** Percent of service availability for the month.
- **Service Availability (12-month average):** Average percent of service availability for the prior 12 months.

EUCC Instant Messaging

- **Service Availability (monthly):** Percent of service availability for the month.
- **Service Availability (12-month average):** Average percent of service availability for the prior 12 months.

Audio, Video and Net Conferencing

- **Service Availability (monthly):** Percent of service availability for the month.
- **Service Availability (12-month average):** Average percent of service availability for the prior 12 months.

Facility Services

Service Description Overview

MN.IT Service's portfolio of Facility Information Technology Services (FIT Services) supports business requirements for the provisioning and management of IT equipment and services in areas such as:

- Common areas – including reception areas, lobbies, elevator areas and hallways
- Conference rooms – including specialized meeting spaces such as board rooms, collaboration spaces, video conference rooms, press conference rooms or demonstration areas
- Training rooms and laboratory areas

FIT Services are focused on:

Facility IT Operations - MN.IT staff supports hardware, software, network, security, and programming features of audio-visual (A/V) technology used to meet Agency business requirements.

Facility IT Design and Development - MN.IT staff works collaboratively with Agency business units and/or vendor-partners to analyze needs, goals, and budget in order to define the best facility IT solutions for the Agency.

In support of its services, MN.IT will de**v**elop and maintain Minnesota standards and vendor contracts for A/V products in major categories that can be used when selecting the facility's IT products. MN.IT will also maintain professional service contracts with vendors that specialize in design and development of A/V systems.

Service Metrics

Support Hours

FIT Service Support is provided during normal business hours.

Service Availability

Due to the wide variety of service components, FIT Service availability is not measured on an overall basis. Availability metrics are defined for individual FIT components based upon Agency business requirements.

Incident Response Levels

The incident response levels associated with FIT Services match those identified in the Service Desk "Incident Management Quick Reference." The following table lists examples of service incidents and the priority levels associated with them.

Table 10: Incident Response Level Examples for FIT Services

Level	Example
Priority 4: Low	• The service is not operational for one or more users outside of the hours of availability.
Priority 3: Medium	• A major function of the service is reported as non-operational during Downtime Period. • Enhancement requests
Priority 2: High	• A minor function of service is not operational for one or more users (who can continue to use other service functions). • A user has questions about the service functionality or needs assistance in using the service. • A user needs administrative assistance.
Priority 1: Critical	• The service is not operational for multiple users during scheduled availability. • A major function of the service is not operational for multiple users during the hours that the service is scheduled for availability.

Service Level Objectives

The tables below contain the Service Level Objectives for the FIT Operational Services.

Table 11: Service Level Objectives for FIT Operations Service

Metric	Definition	Threshold
Service Availability	Measures service availability. **Does not include downtime for scheduled maintenance*	Does not apply
Customer Satisfaction	Measures how the customer perceives the value.	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident response by the Service Desk.	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours

Table 12: Service Level Objectives for FIT Design and Development Services

Metric	Definition	Threshold
Service Response	Measures the time necessary to respond to a typical inquiry regarding the capabilities and availability of professional services staff.	2 business days
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys

Reporting

MN.IT staff for FIT services will develop and support a FIT service reporting process that reflects the needs and resources of the Agency.

Reporting for FIT Design and Development will include:

- Project Hours: Project hours completed and project hours remaining.
- Project Deliverables: Project management tracking via deliverable reporting.
- Project Status/Schedule: Overall project management status and schedule adherence.

Minnesota Geospatial Information Office (MnGeo)

Service Description Overview

The MnGeo Services delivered by MN.IT Services consist of four distinct offerings:

- Geospatial Coordination Services
- Web Services
- Geospatial Professional Services
- Geospatial Commons
- Geospatial Infrastructure Hosting

The sections below provide a high-level description of these services.

Geospatial Coordination Services

As specified in legislation and supported by a legislative appropriation, MnGeo provides coordination services that support the development, implementation and use of geospatial technology in Minnesota. Guided by state agencies, other government and non-government stakeholders, its coordination activities focus on six core activities: community outreach, communications, geospatial data and technology coordination, data and web services, training and technical guidance

Web Services

MnGeo provides multiple web services, including but not limited to:

- Imagery Service: MnGeo's Geospatial Image Service provides versatile access to Minnesota air photos, hillshades, and scanned topographic maps using a Web Map Service (WMS).
- Geocoding Service: MnGeo provides a secure "cascading" geocoding service for use in ArcGIS software and web applications. The service includes data layers for parcel points, address points, street centerlines, city centroids and 5 digit zip code centroids. The service is available only to state agencies for internal applications.

Geospatial Professional Services

MnGeo offers a diverse set of GIS professional services on a fee-for-service basis. MnGeo staff work closely with its clients to define a suitable scope for the service, identify tasks and deliverables, create and refine a work plan and budget, execute and manage the defined effort to completion. Typical client needs require a mix of project design, database development, applications development, spatial analysis and map production. Efforts vary in length and complexity, with some taking a few hours and costing little and others extending over several years and involving significant expenditures. Core geospatial services include providing assistance for developing business requirements, designing solutions, system development/implementation and system operations/maintenance. Professional map printing is also available for existing content.

Geospatial Commons

The Minnesota Geospatial Commons is a collaborative place for users and publishers of geospatial resources in Minnesota. It is powered by The Minnesota Geospatial Information Office (MnGeo), a program of MN.IT Services, the State of Minnesota's single provider of Information Technology.

The Minnesota Geospatial Commons is primarily for geospatial data consumers: People who need data for a project, services for an application, or some other resource required for a GIS-based use. It will be a robust data distribution site that can be used by both traditional and non-traditional GIS users, such as web developers, journalists and others. The Minnesota Geospatial Commons is not intended to provide web mapping functionality like "Google Maps" or "ArcGIS Online."

Geospatial Infrastructure Hosting

Datasets can be stored and will eventually be consolidated at the common infrastructure. Every dataset (or app, or service) must have a metadata record. In addition to the metadata record, a few other pieces of information are required. In the current Minnesota Geospatial Commons model, these additional pieces of information are stored in a Geospatial Data Resource Site (GDRS). Together the metadata records and the GDRS data "feed" the content of the site. Many state agencies already store their data and metadata in a GDRS; however, many organizations that would like to contribute to the Minnesota Geospatial Commons do not yet have, or might not want to set up a GDRS. For this reason, the ability to publish data on the MnGeo Infrastructure will be accomplished in stages, with different steps required for each stage. Input from potential data publishers will help determine the exact requirements.

Geospatial Infrastructure Hosting Service for development, test and production environments includes: server hosting and management, geospatial application hosting and support, and geospatial data hosting

Service Metrics

Support Hours

MnGeo provides Geospatial Coordination and Geospatial Professional Services support during normal business hours.

Support for Geospatial Commons and Geospatial Infrastructure Hosting services is provided 24 x 7 x 365.

Service Availability

Service availability describes the time professional services are available to the Agency. Service availability for professional services varies with staffing levels and project commitments. MN.IT provides clear and timely information on when professional services staff are available.

Incident Response Levels

The incident response levels associated with Security Services match those identified in the Service Desk "Incident Management Quick Reference." The following table lists examples of service incidents and the priority levels associated with them.

Table 13: Incident Response Levels for MnGeo Services

Level	Example
Priority 4: Low	• The service is not operational for one or more users outside of the hours of availability
Priority 3: Medium	• A major function of the service is reported as non-operational during Downtime Period • Enhancement requests
Priority 2: High	• A minor function of the service is not operational for one or more users (who can continue to use other application functions) • A user has questions about the service functionality or needs assistance in using the service • A user needs administrative assistance
Priority 1: Critical	• The service is not operational for multiple users during scheduled availability • A major function of the service is not operational for multiple users during the hours that the service is scheduled for availability • Security Services has identified a breach of a critical system

Service Level Objectives

Service Level Objectives are focused on Geospatial Commons and Geospatial Infrastructure Hosting services. The tables below contain the Service Level Objectives.

Table 14: Service Level Objectives for MnGeo Services

Metric	Definition	Threshold
Customer Satisfaction	Measure how the customer perceives the value	80% positive approval rating through customer surveys
Service Availability	Measures service availability. Combined with other metrics, gives an end-to-end view of geospatial systems as a managed service	99.9% availability* *not including Downtime for scheduled maintenance
Support Response	Measure the speed of incident response by the MN.IT Service Desk	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Request	Measure the maximum time required to respond to a request	Typical – 1 business day Critical – 4 hours

Server Provisioning	Measure the maximum time required to provision for existing customers with all requirements provided, includes VM Server, GIS software, Network Setup	Typical – 4 business days

Reporting

MN.IT MnGeo Services creates reports that meet business requirements. Reports generated from MnGeo Services are made available to customers quarterly.

MnGeo Project Coordination/Professional Services

- **Project Hours:** Project hours completed and project hours remaining
- **Project Deliverables:** Project management tracking via deliverable reporting
- **Project Status/Schedule:** Overall project management status and schedule adherence

Geospatial Commons/Infrastructure Hosting Services

- Service Availability: System uptime
- Support Response: Speed of incident response by priority

Security Services

Service Description Overview

The Security Services delivered by MN.IT Services contain five distinct service offerings:

- Information Security Program Management
- Identity and Access Management
- Information Security Incident Response and Forensics
- Information Security Training and Awareness

The sections below provide a high-level description of these services.

Information Security Program Management

The State of Minnesota recognizes that information is a critical asset. How information is managed, controlled, and protected has a significant impact on the delivery of state services and is vital to maintaining the trust of those that provide data to the State and/or use state programs. Information assets held in trust by the State must be protected from unauthorized disclosure, theft, loss, destruction, and alteration. Information assets must be available when needed, particularly during emergencies and times of crisis.

It is for this reason that Minnesota Statutes chapter 16E requires the State Chief Information Officer (State CIO) to develop cyber security policies, standards, and guidelines for the executive branch Minnesota Statutes also give the State CIO authority to install and administer security systems for use by all.

Key service tasks include:

- Align security program activities and staff with a generally accepted best practice framework
- Oversee the creation and maintenance of information security policies, standards, procedures, and guidelines
- Create and maintain strategic and tactical plans
- Coordinate the movement of plans, policies, standards, and other authoritative documents through a governance process
- Track information security risk key performance indicators
- Disseminate security metrics and risk information to executives and other managers for decision making
- Coordinate security efforts with local government entities and other branches of government

Identity and Access Management

Identity and Access Management manages the identities for users and devices, and controls access to system resources based on these identities, while ensuring users and devices have access to only those systems for which they are properly authenticated and authorized to access.

Key service tasks include:

- Maintain identities by adding/removing user accounts, verifying access to information, etc.
- Enforce password policies ensuring password strength is adequate and resetting within required timeframes
- Manage access to information resources and data, e.g. segregation of duties
- Manage privileged accounts that can bypass security so systems are secure
- Manage encryption keys and security certificates to provide trust for transactions and websites

Information Security Incident Response and Forensics

Information Security Incident Response and Forensics are professional services that utilize multiple tools to resolve the Agency business issues below. Security Incident Management is a process to stop unwanted activity, limit damage, and prevent recurrence of security events. Computer Forensics is a standardized process to determine the cause, scope, and impact of incidents and limit damage that may be used in legal or human resource actions.

Computer Forensics service is often requested separately for investigations that are not part of security incident. Also, this service can be dependent on resources outside the span of control of the service team; these dependencies are identified in the forensics plan, and can affect the ability to meet the service objectives.

A typical investigation takes approximately three weeks to complete due to the data imaging and other investigative best practice processes.

Issues addressed by these services include the following:

- Agency-Specific Incidents
- Denial of Service
- Policy Violations which include Human Resources and Security
- Malware
- Physical Loss/Theft/Damage
- Unauthorized Access
- Unauthorized Alteration/Destruction
- Unauthorized Disclosure

Information Security Training and Awareness

Information security training and awareness provides employees at all levels with relevant security information and training to lessen the number of security incidents.

MN.IT Services can provide training and support in the following areas:

- Generalized Security and Awareness
- Customized Security Training and Awareness for unique requirements
- Online training for SANS Securing the Human which is mandatory for all MN.IT Staff

Service Metrics

Support Hours

Support for Information Security Program Management is provided during

normal business hours

Support for Identity and Access Management services is provided 24 x 7 x 365.

Support for Security Incident Response is provided 24 x 7 x 365.

Computer Forensics is provided during normal business hours

Support for Security Training and Awareness provided during normal business hours

Service Availability

Service availability describes the time professional services are available to the Agency. Service availability for professional services varies with staffing levels and project commitments. MN.IT provides clear and timely information on when professional services staff are available.

Incident Response Levels

The incident response levels associated with Security Services match those identified in the Service Desk "Incident Management Quick Reference." The following table lists examples of service incidents and the priority levels associated with them.

Table 15: Incident Response Levels for Security Services

Level	Example
Priority 4: Low	• The service is not operational for one or more users outside of the hours of availability
Priority 3: Medium	• A major function of the service is reported as non-operational during Downtime Period • Enhancement requests
Priority 2: High	• A minor function of the service is not operational for one or more users (who can continue to use other application functions) • A user has questions about the service functionality or needs assistance in using the service • A user needs administrative assistance
Priority 1: Critical	• The service is not operational for multiple users during scheduled availability • A major function of the service is not operational for multiple users during the hours that the service is scheduled for availability • Security Services has identified a breach of a critical system

Service Level Objectives

Service Level Objectives are focused on the following elements within each Security Service area. The tables below contain the Service Level Objectives for the specified Security Services.

Table 16: Service Level Objectives for Information Security Program Management Service

Metric	Definition	Threshold
Support Resolution	Measure the time necessary to respond to a typical inquiry regarding the capabilities and availability of professional services staff	2 business days
Customer Satisfaction	Measure how the customer perceives the value	80% positive approval rating through customer surveys

Table 17: Service Level Objectives for Identity and Access Management Service

Metric	Definition	Threshold
Customer Satisfaction	Measure how the customer perceives the value	80% positive approval rating through customer surveys
Service Response	Measure the speed of incident response by the MN.IT Service Desk	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Request	Measure the maximum time required to respond to a request.	Typical – 1 business day Critical – 4 hours

Table 18: Service Level Objectives for Information Security Incident Response and Forensics Service

Metric	Definition	Threshold
Service Response	Measure the time necessary to respond to a typical inquiry regarding the capabilities and availability of professional services staff	Target: Next business day Typical: 4 hours
Customer Satisfaction	Measure how the customer perceives the value	80% positive approval rating through customer surveys

Table 19: Service Level Objectives for Security Training and Awareness Service

Metric	Definition	Threshold
Support Resolution	Measure the time necessary to respond to a typical inquiry regarding the capabilities and availability of professional services staff	2 business days
Customer Satisfaction	Measure how the customer perceives the value	80% positive approval rating through customer surveys

Reporting

MN.IT Security Services creates reports that meet business requirements. Reports generated from Security Services are classified as nonpublic and must be handled as such.

- Information Security Program Management: The MN.IT IT Standards and Risk Management Division will assess risk by compiling and reporting metrics for all security services. Details of each service metric and reporting are in the Information Security Program Management Service Description.
- Identity and Access Management: reports for control metrics are created and made available to authorized Agency representatives.
- Security Incident Response and Forensics: Security Incident and Forensic reports are created to satisfy specific inquiry requirements and available to authorized Agency representatives upon request. For the service, volume metrics and time-to-close are also reported.
- Security Training and Awareness: Security Training and Awareness reports can be created to satisfy specific requirements upon request.

.

Voice Services

Service Description Overview

Voice Services consist of the following service categories and are provisioned in one of three ways – through MN.IT infrastructure or through telephone companies or other providers:

- **Dial tone services** provide connections to the public switched telephone network (PSTN). Telephone equipment is provided by MN.IT Services to agencies. Dial tone services include:
  - Classic Voice – telephone lines and telephone numbers of various types, analog or digital circuits, 911 access services and long distance services, contracted through third-party telephone companies.
  - Private Branch Exchange Systems (PBXs) of various types, including Enterprise IP Telephony (IPT) and individual premise-based systems that are analog, digital or IP-enabled.
- **Voice-related applications or services**, including but not limited to:
  - Voicemail – automatic phone messaging and simple menus that answer or direct incoming phone calls.
  - Contact/call center infrastructure that supports telephone call queuing, monitoring and reports for agents that interact with inbound and outbound callers using voice and/or web chat.
  - Interactive voice response (IVR) – menus that answer incoming telephone calls to provide information (optionally connected to external computer systems), transfer calls to call centers based on caller input, and perform other sophisticated functions.
  - Value-added applications for Enterprise IPT – call recording, quality monitoring, workforce management, mobility support and notification/alerting.
  - Over-the-phone interpretation services in which the end user interacts with a limited English proficiency (LEP) citizen by accessing an interpreter for any language.
  - e-Fax services – inbound and outbound fax that provides individual fax telephone numbers for users and can replace the need for fax machines.

Service Metrics

Support Hours

Support hours for Dial Tone Services are:

- **Classic Voice –** 24 x 7 x 365
- **Private Branch Exchange Systems (PBXs) –** 24 x 7 x 365

Support hours for Voice-related applications or services:

- **Voicemail –** 24 x 7 x 365
- **Contact/call center infrastructure –** 24 x 7 x 365
- **Interactive voice response (IVR) –** 24 x 7 x 365
- **Over-the-phone interpretation services –** normal business hours
- **e-Fax services –** 24 x 7 x 365

Service Availability

Service availability represents the percentage of time that a service is running and available to the end-user. The Service Availability metric is derived for each Agency endpoint as a measure of the uptime. Uptime is the time period during which the Service Element at the Agency endpoint and the shared infrastructure is fully functional. Service Availability is calculated as a percentage as shown in the formula below.

$$\frac{[\text{Applicable days in calendar month} \times 24 \times 60] \text{ Minus } [\text{Minutes of outage in calendar month}]}{\text{Applicable days in calendar month} \times 24 \times 60} \times 100$$

When a service is interrupted, Outage is calculated from the time of entering Service Desk incident ticket to the time the ticket is resolved. Downtime Period is a period of ten consecutive minutes of Downtime. Intermittent downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

Service interruption for scheduled maintenance, called Scheduled Downtime, is excluded from the Availability calculation. Scheduled maintenance means those instances when MN.IT notifies the Agency at least five days prior to the commencement of such Scheduled Downtime. The Agency may request the MN.IT Service Desk to reschedule the maintenance if the date and time announced in the notification are not acceptable. MN.IT will work with all agencies to find a suitable date and time for the scheduled maintenance. There will be no more than fifteen hours of Scheduled Downtime per calendar year, and no more than two hours per month. Scheduled Downtime reports will be available to agencies every month.

Incident Response Levels

The incident response levels associated with Voice services match those identified in the Service Desk "Incident Management Quick Reference." The following table lists examples of service incidents and the priority levels associated with them.

Table 21: Incident Response Levels for Voice Services

Level	Example
Priority 4: Low	• Dial Tone Services – minor incidents that do not affect overall functionality • Voice Related Services – minor incidents that do not affect overall functionality
Priority 3: Medium	• Dial Tone Services – telephone service for individual user is non-functional • Voice Related Services – a service for an individual user is non-functional

Level	Example
Priority 2: High	• Dial Tone Services – telephone services for a group of users is non-functional • Voice Related Services – a service is non-functional for multiple users
Priority 1: Critical	• Dial Tone Services – telephone services for a large group of users is non-functional • Voice Related Services – a service is non-functional for all users

Service Level Objectives

The tables below contain the Service Level Objectives for Voice Services.

Table 22: Service Level Objectives for Dial Tone Services

Metric	Definition	Threshold
Service Availability – Classic Voice	Measures the availability for MN.IT Enterprise Classic Voice services.	99.9% availability* *not including Downtime for scheduled maintenance
Service Availability – PBX	Measures the availability for MN.IT Enterprise IPT services.	99.9% availability* *not including Downtime for scheduled maintenance
Customer satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Average time to resolve an incident	Measures the speed of incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Average time to fulfill a move, add, change request for Classic Voice services	Measures the speed of request resolution by MN.IT Services	5 business days
Average time to fulfill a move, add, change request for PBX services	Measures the speed of request resolution by MN.IT Services	5 business days
Average time to fulfill a new implementation request for Classic Voice services	Measures the speed of request resolution by MN.IT Services	12 business days
Average time to fulfill a new implementation request for PBX	Measures the speed of request resolution by MN.IT Services	90 business days

Metric	Definition	Threshold
services		
PBX Call Quality	See service definition for more information	Mean Opinion Score 4 to 5

Table 23: Service Level Objectives for Voice Related Services

Metric	Definition	Threshold
Service availability	Measures the availability for MN.IT Enterprise services.	99.9% availability* *not including downtime for scheduled maintenance
Customer satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Average time to fulfill a move, add, change request for Voice-Related services	Measures the speed of request resolution by MN.IT Services	5 business days
New service implementation response time	Measures the time necessary to respond to a typical inquiry	2 business days

Reporting

Online information will be available on a website with secure login that contains the metrics appropriate to services purchased by the Agency. Service reports will also be available on the secure website.

Web Management

Service Description Overview

Web Management services delivered by MN.IT Services consist of services related to the management of web servers, website design, and mechanisms to manage web content. The sections below provide a high-level description of these Web Management services:

- Web Server Management
- Website Design
- Content Management

Web Server Management

- **Static Web Hosting:** Static web hosting provides storage and delivery of manually updated websites. The service gives agencies a secure, reliable web presence with a specific domain name and covers the processes involved in establishing and maintaining a new static website.
- **Dynamic Web Hosting:** Dynamic web hosting provides a website that delivers real-time, query-based web content. Websites are created using web content management (WCM) tools that are easier to build and maintain than static websites, ensure compliance with web standards, and standardize navigational tools for users. WCM hosting offers a full portal tool suite, including content management, consistent look-and-feel templates and policies, decentralized content creation and posting, agency personalization, and a customized search interface.
- **Website Management Operations:** The delivery of both static and dynamic web hosting services depends on a robust, highly-available infrastructure. MN.IT staff maintains this infrastructure using best practices for equipment maintenance, redundancy, data integrity, security, alerts, and logging.

Website Design

- **User Interface Design:** MN.IT's professional web design staff helps organizations develop a consistent, intuitive, professional browsing experience from a customer-centric perspective. Specific capabilities may include: logo development for fresh agency branding, customer-oriented site navigation and taxonomies, advanced search and metadata development, graphics design, and meeting facilitation for the requirements gathering process.
- **Accessibility:** MN.IT provides assistance with meeting the compliance requirements of both Section 508 and Web Content Accessibility Guidelines (WCAG) 2.0 at the AA level, as well as ADA sections on access to information on state government websites

- **Information Architecture:** Website design services may include information architecture definition related to the integration of visual design, taxonomy development, keywords, naming conventions, and find-ability.

Web Content Management

- **Training:** MN.IT's web hosting and design services may require Agencies to learn new skills to manage/maintain their web content. Typically, MN.IT provides separate training for web content managers and content contributors.
- **Migration Services:** When moving from one hosting platform and/or web technology to another, MN.IT provides tools and techniques for efficiently migrating web content. Depending on the quality of the code, source and destination hosting platforms, migration services may be automated.

Service Metrics

Support Hours

Support for web server management services is provided 24 x 7 x 365.

Support for Web Management (WM) professional services (design and content management) is provided during normal business hours.

Service Availability

Service availability describes the time the system is running and available to the Agency. Service availability for web server management is 99.9% and excludes time to perform routine or scheduled maintenance. Hosting service availability is calculated as follows:

$$\frac{[\text{Applicable days in calendar month} \times 24 \times 60] \text{ minus } [\text{Minutes of outage in calendar month}]}{\text{Applicable days in calendar month} \times 24 \times 60} \times 100$$

Service availability for Web Management professional services varies with staffing levels and project commitments. MN.IT provides clear and timely information on when professional services staff are available.

Scheduled downtime means those times where MN.IT notifies agencies of periods of Downtime for Scheduled Maintenance at least five days prior to the commencement of such Downtime. There will be no more than fifteen hours of Scheduled Downtime per calendar year, and no more than two hours per month. Scheduled Downtime is not considered Downtime for purposes of this SLA, and will not be counted towards any Downtime Periods.

Downtime period is a period of ten consecutive minutes of Downtime. Intermittent Downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

Scheduled Downtime will be announced every month and be available to agencies. If a Scheduled Downtime conflicts with other activities/operations of an Agency, the Agency can

request an alternate date for the Scheduled Downtime thru the service desk. MN.IT will work with all agencies to find a date that balances the needs/priorities of all.

Incident Response Levels

The incident response levels associated with Web Management services match those identified in the Service Desk "Incident Management Quick Reference." The following table lists examples of service incidents and the priority levels associated with them.

Table 24: Incident Response Levels for Web Management

Level	Example
Priority 4: Low	• The hosting service is not operational for one or more users outside of the hours of availability
Priority 3: Medium	• A major function of the hosting service is reported as non-operational during Downtime Period • Enhancement requests
Priority 2: High	• A minor function of the hosting service is not operational for one or more users (who can continue to use other application functions) • A user has questions about the hosting service functionality or needs assistance in using the service • A user needs administrative assistance
Priority 1: Critical	• The hosted website is not operational for multiple users during scheduled availability • A major function of the hosting service is not operational for multiple users during the hours that the service is scheduled for availability

Service Level Objectives

The table below contains the Service Level Objectives for Web Management.

Table 25: Service Level Objectives for Web Server Management

Metric	Definition	Threshold
Service Availability	Measures service availability. *Does not include downtime for scheduled maintenance	99.9% availability*
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident response by the Service Desk	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours

Metric	Definition	Threshold
Server Response	Measures the maximum time before the web server generates a response. **Does not include network latency	0.5 seconds**
Content Change	Measures the maximum time required to make a content change.	Typical – 1 business day Critical – 4 hours

Table 26: Service Level Objectives for Web Design and Content Management

Metric	Definition	Threshold
Support Resolution	Measures the time necessary to respond to a typical inquiry regarding the capabilities and availability of professional services staff.	2 business days
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys

Reporting

Reports for Web Management services are created monthly and made available to agencies. Specific reporting deliverables are listed below:

Static Hosting

- **Hits:** Unique page impressions
- **Data Storage:** Amount of stored data, measured in gigabytes
- **Bandwidth:** Amount of network bandwidth consumed, measured in gigabytes/month
- **Service Availability (monthly):** Percent of service availability for the month
- **Service Availability (12-month average):** Average percent of service availability for the prior 12 months

Dynamic Hosting

- **Hits:** Unique page impressions
- **Data Storage:** Amount of stored data, measured in gigabytes
- **Bandwidth:** Amount of network bandwidth consumed, measured in gigabytes/month
- **Content Items:** Number of items that can be delivered as dynamic content
- **Service Availability (monthly):** Percent of service availability for the month
- **Service Availability (12-month average):** Average percent of service availability for the prior 12 months

Professional Services

- **Project Hours:** Project hours completed and project hours remaining
- **Project Deliverables:** Project management tracking via deliverable reporting
- **Project Status/Schedule:** Overall project management status and schedule adherence

Workstation Management

Service Description Overview

Workstation management is comprised of: 1) operating systems; 2) hardware; 3) software; 4) accessories and peripherals; and 5) security. This section provides a high-level description of the services which comprise Workstation Management delivered by MN.IT Services.

- **Operating Systems**: Microsoft Windows client operating system is the primary supported operating system. Limited support for Mac OS 10.x is also available.
- **Hardware**: A standard laptop, desktop and/or virtual desktop interface device for end users to complete their work. Advanced options within each hardware class may be available, to provide additional computing power (e.g., processor, memory).
- **Software**: Workstations will have "standard" software (e.g., Microsoft Office) installed for end users to complete their work. Beyond what is provided in standard, some end users will require "additional" software which consists of common requested software (e.g., Microsoft Visio) and unique "one-off" software.
- **Accessories and peripherals**: A black and white printer will be made available to all end users and a color printer to those who require one. For those with business needs, specialized and/or accessibility equipment such as audio recording devices, digital cameras, scanners, and screen readers can be purchased on an as needed basis.
- **Security:** Workstations will be configured to install updates and patches on a regular basis, be protected by up-to-date anti-virus software, as well as a local firewall and encryption running on the client operating system.

Service Metrics

Support Hours

Support for Workstation Management is provided during normal business hours.

Service Availability

Service availability describes the percentage of time that the service is running and available to the end user. Service availability for Workstation Management supporting infrastructure is 99.9%. Workstation Management supporting infrastructure includes access to file shares; print servers; critical Windows client patches; and definition updates for anti-virus and anti-malware products. There is no Service Availability metric for end user workstations or workstation accessories and peripherals.

Workstation Management supporting infrastructure service availability is calculated as follows:

$$\frac{[\text{Applicable days in calendar month} \times 24 \times 60] \text{ minus } [\text{Minutes of outage in calendar month}]}{\text{Applicable days in calendar month} \times 24 \times 60} \times 100$$

Scheduled downtime means those times where MN.IT Services notifies agencies of periods of Downtime for Scheduled Maintenance at least five days prior to the commencement of such Downtime. There will be no more than fifteen hours of Scheduled Downtime for Workstation Management per calendar year, and no more than two hours per month. Scheduled Downtime is not considered Downtime for purposes of this SLA, and will not be counted towards any Downtime Periods.

Downtime period is a period of ten consecutive minutes of Downtime. Intermittent Downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

Scheduled Downtime will be announced every month and the schedule will be available to agencies. If a Scheduled Downtime conflicts with other activities/operations of the Agency, the Agency can request an alternate date for the Scheduled Downtime through the MN.IT Service Desk. MN.IT Services will work with agencies to find a date that balances the needs/priorities of all.

Incident Response Levels

The incident response levels associated with Workstation Management match those identified in the Service Desk "Incident Management Quick Reference." The following table lists examples of service incidents and the priority levels associated with them.

Table 27: Incident Response Levels for Workstation Management

Level	Example
Priority 4: Low	• Troubleshooting of one-off "additional" software • Troubleshooting of accessories and peripherals
Priority 3: Medium	• A workstation hardware failure or software error • Troubleshooting of commonly requested "additional" software
Priority 2: High	• A major function of the Workstation Management supporting infrastructure, such as a file or print server unavailable to end users
Priority 1: Critical	• Workstation virus or malware outbreak

Service Level Objectives

The table below contain the Service Level Objectives for Workstation Management.

Table 28: Service Level Objectives for Workstation Management

Metric	Definition	Threshold
Supporting infrastructure availability	Measures service availability of supporting infrastructure (e.g., file shares and print servers, critical Windows client patches).	99.9% availability* *not including Downtime for scheduled maintenance
Customer satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys
Support Resolution	Measures the speed of incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours
Service Response	Measures the speed of request resolution by MN.IT Services	All requests will be entered as "Medium" with 2 business days for resolution, unless specifically listed. Requests can be escalated on a case-by-case basis.
Average time to fulfill Workstation deployment and replacement requests	Measures the speed of fulfilling requests to deploy or replace a workstation ** If workstation and/or resources demands exceed supply, delivery of hardware may impact expected delivery times.	Up to 10 workstations – 10 business days from receipt of hardware** Greater than 10 workstations – delivery time varies**
Average time to fulfill additional "one-off" software requests	Measures the speed of one-off software installation request resolution by MN.IT Services	5 to 10 business days
Critical Windows client patches	Measures the number of workstations receiving timely critical patches/updates.	80% of workstations updated within 7 days

Reporting

Reports for Workstation Management are created monthly and made available to agencies. Specific reporting deliverables are listed below:

- **Laptops:** Total number of laptop computers being supported
- **Desktops:** Total number of desktop computers being supported
- **Total Workstations:** Total number of workstations (e.g., laptop/desktop) being supported

- **User accounts:** Total number of domain user accounts being managed
- **Printers:** Total number of network and local printers/multi-function devices being supported
- **Virus and malware infections detected**: Total number of virus and malware infections detected
- **Operating system by version**: Total number of workstations with a Specific operating system version (e.g., Windows XP, Windows 7 Professional, and Windows Enterprise)

MNsure Standard IT Services Details

General Information

Under "Voice-related applications or services", "e-Fax services" also includes "RightFax services". Under "Service Availability", it's stated that "There will be no more than fifteen hours of Scheduled Downtime per calendar year." This does not include maintenance work required by MN.IT@DHS. Under "Workstation Management", "Limited support for MAC OS 10.x is also available" should be removed. Under "Accessories and peripherals", "MFD" should be added to the list of accessories. The "Reporting" section under Workstation Management should state "Specific reporting deliverables will be made available upon request". Under "Facility Services", it should be noted that MNsure physical security systems are supported in large part by their building's landlord. The systems supported by landlords or 3rd party vendors are not covered by this SLA.

Normal Work Hours

7:30-4:00

Service Metrics

If service level objectives differ from the standards in Section 3, the differences are noted below. If an Agency Threshold is blank, the Standard Threshold applies.

If this section is blank, then all Section 3 Standard Thresholds apply.

Table 2: Service Level Objectives for Wireless Access

Metric	Definition	Standard Threshold	Agency Threshold
Service Availability	Measures the wireless infrastructure service availability	99.9% availability* *not including Downtime for scheduled maintenance	100%
Customer satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys	N/A
Support Resolution	Measures the speed of incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours	Within 1 hour
Service Request	Measures the speed of service response by MN.IT Services	30 minutes for “guest” access; 2 business days for all other requests	Guest - immediate, Employee - 2 business days

Table 3: Service Level Objectives for VPN Remote Access

Metric	Definition	Standard Threshold	Agency Threshold
Service Availability	Measures the VPN Remote Access service availability	99.9% availability* *not including Downtime for scheduled maintenance	100%
Customer satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys	N/A
Support Resolution	Measures the speed of Incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours	Within 2 hours
Service Request	Measures the speed of service response by MN.IT Services	2 business days	2 business days

Table 4: Service Level Objectives for Cellular Service Plans and Devices

Metric	Definition	Standard Threshold	Agency Threshold
Customer satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys	N/A
Support Resolution	Measures the speed of Incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours	
Service Request	Measures the speed of service response by MN.IT Services	5 to 7 business days after Purchase Order (PO) creation	14 business days (5-10 business day) following reciept of a purchase order

EUCC SharePoint services is not provided to MNsure.

Table 9: Service Level Objectives for Audio, Video and Net Conferencing Services

Metric	Definition	Standard Threshold	Agency Threshold
Service Availability	Measures service availability	99.9% availability* *not including Downtime for scheduled maintenance	
Customer satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys	N/A
Support Resolution	Measures the speed of Incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours	2 hours - 5 business days
Service Request	Measures the speed of service response by MN.IT Services	All requests will be entered as “Medium” with 2 business days for resolution, unless specifically listed. Requests can be escalated on a case-by-case basis.	

FIT Design and Development Services is not provided to MNsure.

Table 19: Service Level Objectives for Security Training and Awareness Services

Metric	Definition	Standard Threshold	Agency Threshold
Service Response	Measures time necessary to respond to a typical inquiry regarding the capabilities and availability of professional services staff.	2 business days	
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys	

Table 22: Service Level Objectives for Dial Tone Services

Metric	Definition	Standard Threshold	Agency Threshold
Service Availability - Classic Voice	Measures service availability for Classic Voice services	99.9% availability* *not including Downtime for scheduled maintenance	
Service Availability - PBX	Measures service availability for IPT services	99.9% availability* *not including Downtime for scheduled maintenance	
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys	
Support Resolution	Measures the speed of Incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours	
Service Response for changing Classic Voice	Measures the speed of service response to move, add or change services by MN.IT Services	5 business days	10 business day
Service Response for changing PBX	Measures the speed of service response to move, add or change services by MN.IT Services	5 business days	10 business days
Service Response for New Classic Voice implementation	Measures the speed of service response by MN.IT Services	12 business days	15 business days
Service Response for New PBX implementation	Measures the speed of service response by MN.IT Services	90 business days	
PBX Call Quality	See service definition for more information	Mean Opinion Score 4 to 5	

Table 23: Service Level Objectives for Voice Related Services

Metric	Definition	Standard Threshold	Agency Threshold
Service Availability	Measures service availability.	99.9% availability* *not including Downtime for scheduled maintenance	
Customer satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys	
Support Resolution	Measures the speed of Incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours	
Service Response for changing Voice-Related services	Measures the speed of service response to move, add or change services by MN.IT Services	5 business days	5 business days - 90 business days
New service implementation response time	Measures the time necessary to respond to a typical inquiry	2 business days	

Table 28: Service Level Objectives for Workstation Management

Metric	Definition	Standard Threshold	Agency Threshold
Supporting Infrastructure availability	Measures service availability of supporting infrastructure (e.g., file shares and print servers, critical Windows client patches).	99.9% availability* *not including Downtime for scheduled maintenance	
Customer Satisfaction	Measures how the customer perceives the value	80% positive approval rating through customer surveys	
Support Resolution	Measures the speed of Incident resolution by MN.IT Services	Priority 4: Low - 5 business days Priority 3: Medium - 2 business days Priority 2: High - 8 hours Priority 1: Critical - 2 hours	
Service Response	Measures the speed of service response by MN.IT Services	All requests will be entered as “Medium” with 2 business days for resolution, unless specifically listed. Requests can be escalated on a case-by-case basis.	
Service Response for Workstation deployment and replacement	Measures the speed of service response by MN.IT Services. ** If workstation and/or resources demands exceed supply, delivery of hardware may impact	Up to 10 workstations - 10 business days from receipt of hardware. ** Greater than 10 Work-stations -delivery time varies.	
Service Response for "One-off" Software Installation	Measures the speed of service response by MN.IT Services	5 to 10 business days	
Critical Windows Client Patches	Measures the number of workstations receiving timely critical	80% of workstations updated within 7 days	Patches are piloted on Patch Tuesday, then deployed to environment over 2-3 weeks depending on urgency.

Section 4: Agency Applications

MNsure Applications

Introduction

The MNsure applications section describes the collection of applications that support the agency ’s business processes. In this context, an ‘‘application’’ is software that functions by means of computers to accomplish useful work.

MN.IT Services staff support thousands of different applications enterprise-wide, ranging from Parking Lot Systems to Vendor Management Systems to Web Content Management Systems. These applications may be composed of dedicated hardware and highly customized software, or may be vendor purchased ‘‘commodity’’ products. This section describes these applications, who supports them, how they work, and the relative priority to business users.

The details for each application can vary greatly, so the following standard information has been gathered for each major application in order to facilitate effective analysis and accountability:

- **Business Division**: Primary unit within the agency structure that uses the application
- **Business Purpose**: The logical grouping of applications in support of a Business Purpose or Business Function. Applications will be sorted under each Business Purpose. For example, 10 unique applications are grouped together to provide the features and functions needed to support ‘‘License Renewal’’.
- **Application Name**: How agency staff commonly refer to the application
- **Description**: Description of application
- **Contact**: Business person within the agency that should be contacted for business requirements and additional information about the application
- **Attended Hours of Operation**: Times when the application is available for use and attended by MN.IT staff.
- **Hours of Operation Currently Met**: Indicator of whether or not the Hours of Operation are being achieved with the current level of infrastructure (staff, equipment, contracts, etc.)
- **Recovery Time Objective** (RTO): The maximum period of time available for recovering an application before there is a significant impact on the agency. Possible RTO periods for the purposes of this document are as follows:

  - Immediate (no downtime)
  - 24 Hours
  - 72 Hours
  - 5 Days
  - 2 Weeks (14 Days)
  - 4 Weeks (28 Days)
  - N/A (will not be recovered)
  - 8 Hours
  - 48 Hours
  - 4 Days
  - 1 Week (7 Days)
  - 3 Weeks (21 Days)
  - TBD

- **RTO Achievable**: Indicator of whether or not the RTO can be achieved with the current level of infrastructure in the event of a disaster
- **Criticality**: Impact if the application becomes unavailable because of an unplanned service incident. The criticality levels are as follows:
    - 1 (Critical) = any incident that has "massive impact" and is highly visible, impacts a significant number of users, a major agency, application or service and has no redundancy or alternate path.
    - 2 (High) = any incident that impacts a significant number of users, a major agency application or service, but has redundancy, or an alternate path or bypass.
    - 3 (Medium) = any incident that impacts a limited number of users with a resource or service down or degraded.
    - 4 (Low) = any incident that impacts a small number or a single user in which a resource or non-critical service is down or degraded and a deferred fix or maintenance is acceptable.
- **Availability Service Level %**: Service availability describes the time the system is running and available to the business customer. Availability Service Level is calculated as follows:

$$\frac{\text{Applicable days in calendar month x 24 x 60 minus [Minutes of outage in calendar month]}}{\text{Applicable days in calendar month x 24 x 60}} \times 100$$

Typical service availability levels can be characterized as follows:

- 99.9% - Maximum of 8 hours, 45 minutes of downtime per year. This level requires 24 x 7 staffing, "High Availability" (HA) system design, and redundant components.
- 99.5% - Maximum of 43 hours, 48 minutes of downtime per year. This level requires having staff "on call", spare parts, and/or maintenance contracts for parts delivery.
- 99.0% - Maximum of 87 hours 36 minutes of downtime per year. This level requires having staff "on call", well-defined system recovery procedures, and business hour staffing.

- **Regulatory Compliance Service Requirements**: Listing of any external or internal compliance requirements that govern the application. Examples include: HIPAA, JCAHO, IRS Publication 1075, etc.
- **Information Classification Service Requirements:** Indicator of information classification associated with the application. When multiple classifications apply, the highest classification is applied. Information Classifications are as follows:
    - A = Confidential or Protected Nonpublic
    - B = Private or Nonpublic
    - C = Public

The information provided for each Agency application is presented "as is," meaning that the data has been provided by the Agency-based CIO to reflect current capabilities and characteristics based on available data. As metrics change and/or more application information is available, changes will be incorporated into this document.

Business Division: **MNsure**

Business Purpose: Health Insurance Exchange Solution Set

Application Name: **1) Health Care Reform Identity and Access Management**

Application ID **H60-4 TBD**

Contact: Scott Leitz

Description: MNsure application to support account creation, account management, login, and remote identity proofing.

Attended Hours of Operation:

Monday - Friday	C 8-6 pm
Saturday	C 8-6 pm
Sunday	C 8-6 pm
Holiday	C 8-6 pm

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD

RTO achievable?: TBD

Criticality: Critical

Regulatory Compliance Service Requirements: HIPAA/HiTech, Affordable Care Act, OMB Circular A-133, see Appendix A

Information Classification Service Requirements: Confidential or Protected Nonpublic

Additional Comments:

Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Application Name: **2) Health Care Reform Eligibility (Cúram)**

Application ID **H60-2 TBD**

Contact: Scott Leitz

Description: Worker, citizen, and anonymous shopping portals for MNsure. Functionality provided includes determination of eligibility, individual plan selection, and individual plan enrollment.

Attended Hours of Operation:

Monday - Friday	All Other (Typically 7x24)
Saturday	All Other (Typically 7x24)
Sunday	All Other (Typically 7x24)
Holiday	All Other (Typically 7x24)

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD

RTO achievable?: TBD

Criticality: Critical

Regulatory Compliance Service Requirements: HIPAA/HiTech, Affordable Care Act, OMB Circular A-133, see Appendix A

Information Classification Service Requirements: Private or Nonpublic

Additional Comments:

Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Business Division: **MNsure**

Business Purpose: Health Insurance Exchange Solution Set

Application Name: **3) Health Care Reform Plan Selection (Connecture)**

Application ID **H60-7 TBD**

Contact: Scott Leitz

Description: MNsure applications to support small employer health options program (SHOP) plan selection and navigators/brokers.

Attended Hours of Operation:

Monday - Friday	C 8-6 pm
Saturday	C None
Sunday	C None
Holiday	C None

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD

RTO achievable?: TBD

Criticality: Critical

Regulatory Compliance Service Requirements: HIPAA/HiTech, Affordable Care Act, OMB Circular A-133, see Appendix A

Information Classification Service Requirements: Private or Nonpublic

Additional Comments:

Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Application Name: **4) Health Care Reform Financials (EP Financials)**

Application ID **H60-3 TBD**

Contact: Scott Leitz

Description: MNsure application to calculate premiums, generate billings, record payments, and to process collections and risk adjustment

Attended Hours of Operation:

Monday - Friday	C 8-6 pm
Saturday	C None
Sunday	C None
Holiday	C None

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD

RTO achievable?: TBD

Criticality: Critical

Regulatory Compliance Service Requirements: HIPAA/HiTech, Affordable Care Act, OMB Circular A-133, see Appendix A

Information Classification Service Requirements: Private or Nonpublic

Additional Comments:

Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Business Division: **MNsure**

Business Purpose: Health Insurance Exchange Solution Set

Application Name: **5) Health Care Reform Integration**

Application ID **H60-5 TBD**

Contact: Scott Leitz

Description: Integration and interfaces between MNsure components and other applications. This includes carrier enrollment, document management and archiving, notices and templates, and 2-way interfaces, e.g., MMIS, the federal hub, SWIFT, SMI, etc.) , and an estimated 50 software mediations that include, but are not limited to the components listed in the Additional Comments below.

Attended Hours of Operation:

Monday - Friday	C 8-6 pm
Saturday	C None
Sunday	C None
Holiday	C None

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD

RTO achievable?: TBD

Criticality: High

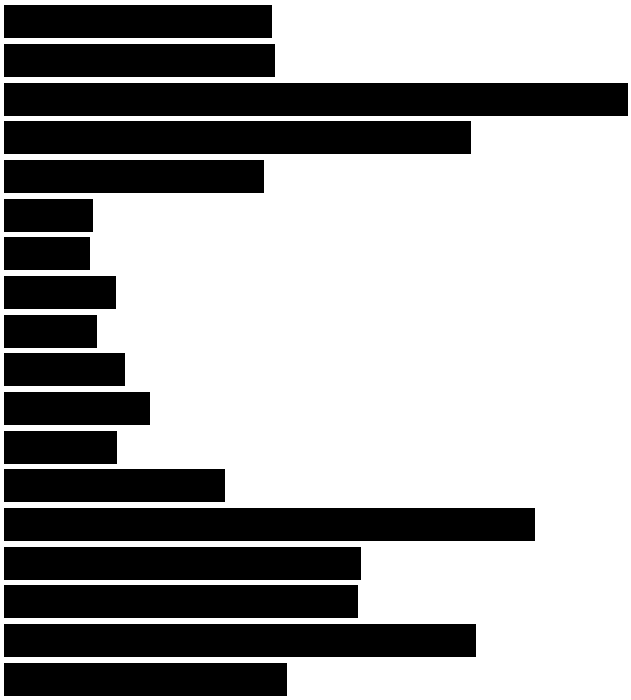
Regulatory Compliance Service Requirements: HIPAA/HiTech, Affordable Care Act, OMB Circular A-133, see Appendix A

Information Classification Service Requirements: Private or Nonpublic

Additional Comments:

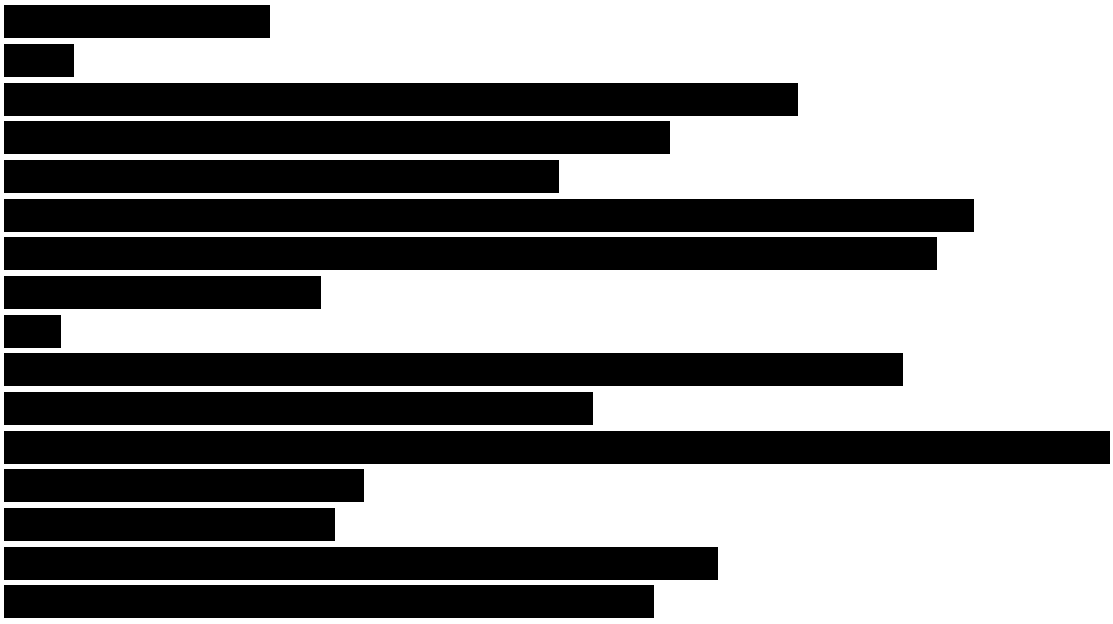
Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Product



Business Division: **MNsure**

Business Purpose: Health Insurance Exchange Solution Set



Application Name: **6) Health Care Reform Reporting** Application ID **H60-6 TBD**

Contact: Scott Leitz

Description: Reporting for MNsure, including web metrics, database reporting and the replicated data store. To date, all reporting is created on an ad hoc basis via technical staff; nothing is automated and little direct access is available to business or policy staff

Attended Hours of Operation:

Monday - Friday	Standard Business Hours (7am - 5pm CST)
Saturday	C None
Sunday	C None
Holiday	C None

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD RTO achievable?: TBD Criticality: Medium

Regulatory Compliance Service Requirements: HIPAA/HiTech, Affordable Care Act, OMB Circular A-133, see Appendix A

Information Classification Service Requirements: Private or Nonpublic

Additional Comments:

Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Business Division: **MNsure**

Business Purpose: Health Insurance Exchange Solution Set

Application Name: **7) Health Care Reform Contact Center Ticketing**

Application ID **H60-1 TBD**

Contact: Scott Leitz

Description: Track calls coming into the MNsure contact center.

Attended Hours of Operation:

Monday - Friday	Standard Business Hours (7am - 5pm CST)
Saturday	C None
Sunday	C None
Holiday	C None

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD

RTO achievable?: TBD

Criticality: High

Regulatory Compliance Service Requirements: Affordable Care Act, OMB Circular A-133,see Appendix A

Information Classification Service Requirements: Private or Nonpublic

Additional Comments:

Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Application Name: **8) MNsure Receipts**

Application ID **H60-9 TBD**

Contact: Linda Froncak

Description: Track MNsure payments at DHS Walk-in Payment Center

Attended Hours of Operation:

Monday - Friday	C 8-6
Saturday	C None
Sunday	C None
Holiday	C None

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD

RTO achievable?: TBD

Criticality: Low

Regulatory Compliance Service Requirements: OMB Circular A-133, see Appendix A

Information Classification Service Requirements: Public

Additional Comments:

Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Business Division: **MNsure**

Business Purpose: Health Insurance Exchange Solution Set

Application Name: **9) MNsure Logo Application**

Application ID **H60-8 TBD**

Contact: Jessica Kennedy

Description: Track and manage requests for use of the MNSure Logo

Attended Hours of Operation:

Monday - Friday	Standard Business Hours (7am - 5pm CST)
Saturday	C None
Sunday	C None
Holiday	C None

Hours of Operation currently met?: No

Availability Service Levels %:

Recovery Time Objective (RTO): TBD

RTO achievable?: TBD

Criticality: Low

Regulatory Compliance Service Requirements: OMB Circular A-133, see Appendix A

Information Classification Service Requirements: Public

Additional Comments:

Work is in progress to determine the appropriate Recovery Time Objective (RTO) for the application, and to test to ensure it's achievable. Once determined the application RTO information will be updated.

Section 5: Projects and Initiatives

Projects and Initiatives

Managing Project Resources and Project Priorities

Historically, most agencies have had a pool of discretionary technology funds to use throughout a budget year for IT initiatives that include the following types:

- **New applications/systems**: The design and building of business applications and tools that perform functions and processes for state programs.
- **Enhancements and changes**: Changes, enhancements and upgrades to existing applications or systems due to changing business needs and/or changing technologies.
- **Ad hoc IT requests**: IT business analysis that does not rise to the definition of a project, but requires some information technology subject matter expertise.

Within its available resources, Agency business leadership has, prior to IT consolidation, been able to manage project resources and priorities on an ongoing basis, based on their business needs and priorities.

The Agency will continue to have that same discretion within this SLA.

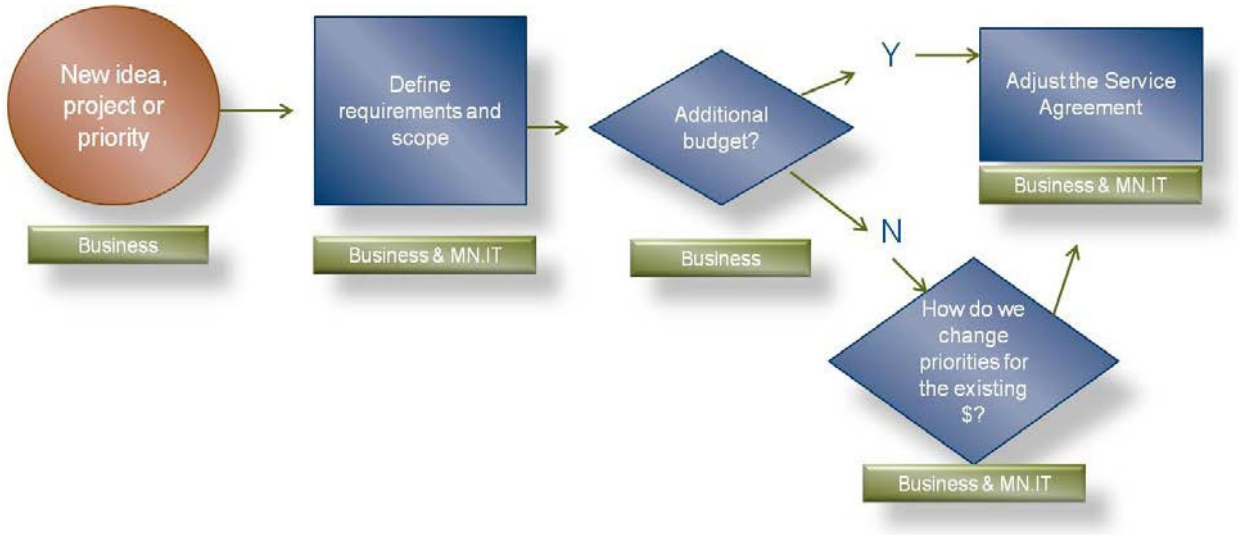
Under the terms of this SLA, the management of IT project resources and project priorities is an iterative process throughout the fiscal year, managed through a cooperative relationship between MN.IT Services and Agency business leadership.

Section 6 of this SLA outlines the portion of the Agency's total technology budget that is currently allocated to projects and initiatives. From this pool of identified funding, the Agency-based CIO will work in consultation with Agency business leadership to set priorities, manage a project portfolio as described above, and regularly report on portfolio status. Should priorities change or should circumstances arise that change available resources, the decision on how resources should be allocated and projects changed is a business decision made by Agency business leadership in consultation with the Agency-based CIO.

When a new initiative is proposed, the Agency business unit and the Agency-based CIO determine the availability of resources within the existing discretionary resource pool described in Section 6. This analysis may result in the need for an Agency executive leadership decision to adjust portfolio priorities or it may require the identification of funding beyond the available resource pool. In such cases, the Agency business unit and Agency-based CIO work to analyze the change's impact on the project portfolio, identify and allocate resources for the proposed project, and amend Section 6 of the SLA as necessary.

The diagram below summarizes the ongoing process by which MN.IT will work with Agency business to reprioritize IT projects and initiatives covered in this section in order to meet the Agency's highest priorities. See Section 1 for IT budget changes ("Acceptance, Amendments,

and Termination”). A more detailed budget change process is being developed and will be distributed when it is complete.



Types of Project and Initiatives

New Applications / Systems

It is not unusual for issues, concerns, challenges or priorities to emerge that require the development of a new application or system within a given fiscal year. Examples might include new legislative requirements, a policy change, or the need to replace a legacy system.

In the case of a new application or system, the Agency-based CIO will work with the appropriate Agency business units to identify the need, requirements, scope, budget, and schedule for a new project, based upon its alignment and contribution to the Agency’s strategies and objectives.

If necessary, the Agency-based CIO will assign project management or business analysis resources to conduct the discovery process that will provide the details necessary for an executive leadership decision on whether to proceed.

With executive leadership approval, the Agency-based CIO will add the project request to the queue as appropriate and assign the appropriate resources to work with the Agency business unit.

Enhancements and Changes

Existing applications and systems often require regular enhancements and changes that keep them current with new technologies, security improvements, and changing business requirements. Although most enhancements and change projects may not be as large, costly

and complex as new system development, they consume significant resources and require the same level of project management discipline as new projects.

The process to analyze the requirements of an enhancement or change project, to assess the project's impact on the project portfolio, and the financial requirements mirror the processes for new projects.

Ad hoc Requests for a Short-term Effort

There will be times when Agency business leadership determine the need for a technical resource for short-term activities or initiatives that do not rise to the level of a formal project. Examples of technical resources that may be needed to augment existing staff include business analysts, network designers, programmers, developers, or architects.

To meet this need, the Agency business unit will work with the Agency-based CIO to determine the best approach for acquiring the appropriate resources. The Agency-based CIO will then facilitate the contracting process utilizing the appropriate procurement process, depending on the resource, i.e., contracting with MN.IT Services, ASAP-IT, or one of the other state contracting mechanisms.

Project Management and Oversight Processes

MN.IT Services provides professional project managers to lead projects from initiation through execution in a manner that meets the priorities of Agency business leadership and the policies and standards of the State for project and portfolio management.

In delivering this service, the assigned project manager will be responsible for the following activities:

- Prepare the project charter, project plan, and project status documents
- Plan tasks, identify resource needs
- Perform project risk management
- Assign planned tasks to staff and contractors assigned to the project
- Monitor progress and regularly report status
- Lead project change management and communications
- Log and track project issues
- Facilitate project-related decision-making
- Cooperate with Agency business unit to facilitate a smooth transition to operational support
- Coordinate with MN.IT Services' Information Standards and Security Risk Management Division to ensure compliance with project management policies, state architecture, accessibility, security and procurement standards, and statutory requirements. The policies are located on the MN.IT website http://mn.gov/oet/programs/policies/
- Manage the project budget

Project Management Policy and Statutory Compliance

In addition to project and program management for Agency-based IT projects, MN.IT Services' Enterprise Project Portfolio Management Division provides services that verify and review the application of project management best practices, policy, and statutory compliance for all Agency-based IT projects. As part of this oversight function, the Enterprise Project Portfolio Management Division meets with the Agency's project manager to determine the appropriate level of oversight required by policy and statutes. The Enterprise Project Portfolio Management Division also assists the project manager with acquiring resources to perform required risk management and project audit activities as needed for projects that meet the thresholds for this requirement.

Requesting Projects and Initiatives

The following pages describe the process by which Agency business units and/or leadership request project and initiatives services or changes at the Agency.

In FY2013, MN.IT Services will be developing a standard process for all project and service requests regardless of location. When that process is available, this Service Level Agreement will be amended to reflect the changes.

MNsure Projects and Initiatives Details

MN.IT @ MNsure Project Management Office (PMO)

The MN.IT@ MNsure PMO has the following processes and procedures related to the services outlined in Section 5: Projects and Initiatives.

General Information

The MN.IT @ DHS/MNsure Project Management Office is an office within the Program Management Division of MN.IT Services @ DHS/MNsure. It is staffed with the MN.IT Services @ DHS project managers, a Portfolio Manager/Relationship Manager, PM supervisors and a PMO manager.

Contact Information

PMO Name	MN.IT Services @ DHS/MNsure PMO
Business Hours	7:30 - 4:00
Contact Name	Mark Broberg
Phone Number	651/431-4993
Email Address	Mark.Broberg@state.mn.us

Project Requests

MN.IT@ MNsure PMO has established the following process or procedure for requesting an IT project:

Projects to develop the MNsure IT System are backlogged through the year and each January, the MNsure Executive Steering Committee prioritizes the backlog of projects to create a plan for the next year. Any change to the projects or plan is submitted through the MNsure IT System Change Control Board.

Other IT project requests submitted through the project request process or the Gateway process include:
1. A business need for a project is identified
2. The MNsure management determines the project need is a priority
3. A Project Request form is completed which will then be routed to the appropriate enterprise architecture team(s) for review.
4. Upon approval, the Project Management Office (PMO) will schedule a meeting with the Requestor and the appropriate IT staff to further define project requirements. The Gateway project request is found here: [redacted].

Project Portfolio Management

MN.IT@ MNsure PMO has established the following process or procedure and governance for prioritizing, authorizing, and monitoring the agency portfolio of IT projects:

The portfolio management process at DHS and MN.IT Services @ DHS/MNsure is a gated process which key principles include: no wrong door, single point of contact, the process should not add excessive time/work to the project, and routine work requests are handled through the service catalog. The process is documented here: [redacted]

Project Management

Project managers use a common set of project management processes, templates and standards which work within the framework set by MN.IT Services statewide. Project managers work the project from initiation through completion and closure using the PM standards found here: [redacted]

Section 6: Service Financial Information

Service Financial Information

Introduction

This section of the SLA defines an agency's total IT budget consisting of the cost of agency- based IT, the cost of enterprise (centrally provided) IT services, biennial IT (BIT), and Odyssey Funds. The FY15 agency IT budget was prepared by the agency CIO's, reviewed by the agency CFO and confirmed with the State CIO.

☐ 3 types of billing will be in effect for FY15:

- Group A (Rates): for those agencies that will be billed based on service rates, the agency-based IT portion of the budget has been recorded in SWIFT on a cash basis and will be invoiced using service rates approved by MMB, using the accrual basis.
- Group A (Direct Charges): for those agencies that will be billed for payroll and non-payroll costs based on MN.IT procurement transactions, agency-based costs will be paid for directly by MN.IT through MN.IT @ agency FinDeptIDs.
- Group B: for those agencies that will be billed for non-payroll costs only based on MN.IT procurement transactions, agency-based costs will be paid for directly by MN.IT through MN.IT @ agency FinDeptIDs. Payroll costs will be paid directly by agencies out of agency FinDeptIDs.

☐ The portion of the budget for enterprise (centrally provided) IT services is based upon forecasted demand and expenses. The billing of centrally provided IT services is based upon application of usage-based and fee-for-service rates approved by MMB.

MN.IT Services has adopted a new service costing model for IT, M-PWR that is used to calculate rates for centrally provided services. The tool is also used to calculate service rates for agency-provided IT services once an agency's IT financial responsibilities are transferred to MN.IT and the agency's local rates are approved by MMB. The use of this tool will be expanded in the future to include calculation of all agency IT rates, budgets, forecasting, and reporting.

Benefits for Business

This analysis and view of current service costs has many benefits for the Agency's business leadership, particularly at the point and time where IT management and responsibility is shifting to a central IT organization. The purpose of this document, therefore, is to help:

- Customers understand and track the costs currently associated with the services they currently get, thus increasing ongoing understanding and accountability for MN.IT Services to the agency customer.
- Agency business leadership use the information to plan and prioritize how information technology serves the business units and priorities of the organization.

Benefits for IT

Service costing has become the standard of the information technology industry and provides many benefits to MN.IT Services in its responsibility to meet the intent of the consolidation law.

- MN.IT can evaluate service costing across all of its agency offices, allowing a global analysis of spending trends, cost fluctuations, and gaps.
- This analysis sets a baseline for setting service delivery standards within a newly consolidated organization, allows a better competitive market comparison for sourcing decisions and identifies opportunities for service improvements and efficiencies.
- The model provides a mechanism for instituting accountability enterprise-wide for service levels and costs, and a foundation for future service level reporting.
- The model provides a baseline for measuring and quantifying future savings as efficiencies are realized over time through consolidated activity.
- Comparing service costs across the enterprise helps to identify areas of under-spending that need to be addressed.
- Aligning costs with services begins for MN.IT Services a “to do” list for systems and asset investment for such issues as legacy systems, security and IT service continuity remedies, etc. and is the foundation for investment prioritization in alignment with the Minnesota IT Master Plan.

More Accurate Data for Improved Decision-Making

There has been continuing progress in the State’s ability to account for how IT dollars are spent across the board. As we have the opportunity to review and analyze the data across all agencies, two important outcomes will emerge:

1) A foundational baseline that will help MN.IT Services to deliver IT more effectively and efficiently across the executive branch.
2) Data that will enable better decision-making at both the agency and stakeholder level on the most effective IT investments for the business of the State.

Evolution of the Costing Model

IT Costing Model: October 2011

As a pre-requisite for meeting the legislative mandate to transfer authority for information technology budgets and personnel to the Office of MN.IT Services, it was necessary first to define the agency dollars that accompanied the change.

To accomplish this by the mandated deadline of October 2011, agency financial staff and leadership worked together with MN.IT to analyze available data and arrive at a definition of the personnel, dollars and activity that would be considered “in scope” for consolidation.

Agency fiscal and leadership staff collected financial information on planned IT Spend for fiscal years 2012 and 2013. This self-reported information was validated against prior years' actual financial reports, IT spend reports, and through in-person interviews with agencies' fiscal and other leadership staff.

The resulting total costs were outlined in the October 2011 interagency agreement that officially transferred authority for the IT budget and personnel.

The October 2011 cost evaluation was a significant step forward in the State's ability to identify and quantify the entire IT spend for the executive branch. It allowed MN.IT and the agency to agree to an acceptable and reasonable level of spending that would meet the agency's needs in an "as is" scenario for FY12.

IT Costing Model: Initial Interagency Agreement/SLA

For this phase of the consolidation, MN.IT Services used the self-reported financials for FY2013 (above) and converted the financial information from an "account code" view to the defined set of services in this Service Level Agreement (**Standard IT Services**, **Applications**, **Projects and Initiatives**). The costing model for each service includes the following:

- **Directly attributable costs**: Costs that are directly attributable to a given service were attributed to that service. Large expenses such as telecom, software, hardware, professional technical contracts, etc., were given greater scrutiny.
- **Allocated costs**: Smaller expenditures, miscellaneous expenses and/or costs that are not clearly attributable to a single service have been allocated across all services by a formula based on the relative size of the service.

IT Costing Model: M-PWR (NICUS)

In March 2013, MN.IT adopted a new IT financial management tool called M-PWR (NICUS). This tool embodies a systematic and integrated approach to performing IT budgeting, cost allocation (service rate development), forecasting, and reporting. The first phase currently being implemented is for service rate development for both centrally provided and agency-based (local) IT costs. Follow-on phases will include budgeting, forecasting, and reporting. An important part of the implementation of M-PWR will be the building of interfaces with statewide systems such as SWIFT, SEMA-4, and BPAS. Some of the key attributes of the cost allocation model are as follows:

- ☐ A new chart of accounts (COA) was established for MN.IT Services based upon a service reference model that allows IT costs to be captured in the appropriate functional "buckets".

- ☐ The cost allocation tool has the ability to then assign these costs directly to individual services - IT standard services, projects, and applications - for a view of costs per service. These services include the underlying infrastructure costs, which are allocated according to established unit volumes/metrics.
- ☐ The rates for a given service are calculated as the sum of direct and indirect allocated costs per the relevant metric (unit volume).
- ☐ Rates are calculated for centrally provided services as well as for agency-based IT services for a combined service total to be billed back by MN.IT Services.
- ☐ Initially, the NICUS tool will be used to verify and provide a showback invoice to agencies for their service costs but will not be the official billing tool until implementation of the system is complete. Until that time,
    - o All agencies will continue to receive three invoices for enterprise (centrally provided) services through the existing billing system: Computing, WAN, and Voice.
    - o Agencies that have transferred financial responsibility to MN.IT Group A (Rates) will also receive a bill for locally provided services based on actual volumes times budgeted rates, as approved by MMB.
    - o Agencies that have not yet transferred financial responsibility to MN.IT will have their agency-based office expenses paid directly by MN.IT and assigned to MN.IT @ Agency FINDeptIDs.
        - Group A (Direct Charges) agencies will have payroll and non-payroll costs paid out of MN.IT FinDeptIDs,
        - Group B agencies will only have non-payroll costs paid out of MN.IT FinDeptIDs. Payroll costs will be paid out of agency FinDeptIDs with IT attributes... These agencies will also receive a “showback” invoice during FY15 that will provide a view of their IT service costs.

Service Billing and Procurement

This document does not represent an invoice. It is an accounting of the Agency’s current IT budget by account classification for agency-based IT and a single line item for centrally provided IT services based upon an agency forecast.

The financials contained in this SLA include all IT, regardless of source, including those services provisioned at the Agency, centrally and/or by a third party.

Agency-specific services: All Agency-specific IT service activity and expenditures will be managed by the Agency-based CIO within the Agency’s identified IT budget.

Centrally provided MN.IT services: Services managed and/or provided centrally will be billed to the Agency by MN.IT Services, based on the published FY14 rate package. Costs for such services have been accounted for and will go against the Agency's IT budget, like all other costs.

Payment Terms:
Statute 16A.124 PROMPT PAYMENT OF STATE AGENCY BILLS REQUIRED.
"**Subd. 1a.State agencies are vendors**. For purposes of this section, a state agency that bills another state agency for a service or commodity is considered a vendor like any nonstate vendor.
Subd. 3. Payment required. State agencies must pay each valid vendor obligation so that the vendor receives payment within the vendor's early payment discount period. If there is no early payment discount period, the state agency must pay the vendor within 30 days following the receipt of the invoice for the completed delivery of the product or service.
Subd. 4.Invoice errors. If an invoice is incorrect, defective, or otherwise improper, the agency must notify the vendor within ten days of discovering the error. Upon receiving a corrected invoice, the agency must pay the bill within the time limitation contained in subdivision 3."

In the event of a dispute on certain items on an invoice, agency shall pay for the non-disputed items within 30 days from the receipt of the invoice. For disputed items, MN.IT and agency shall follow the Dispute Resolution process outlined in Section 1.

Notice of Cancellation: "Agencies will provide at least 30 days' notice to MN.IT@agency of cancellation of projects and termination of services In order to avoid unnecessary costs being incurred and to have the ability to properly reallocate resources."

Procurement: Procurement of IT commodities and IT contracts commenced on **J**uly 1, 2013 for agencies whose finances were consolidated, and by the end of the second quarter, FY14 for most other executive branch agencies. For consolidated agencies, the purchases will be coded in the MN.IT chart of accounts such that they will be accounted for in the individual agency-based office IT Spend. For agencies that have not yet consolidated their IT finances, purchases will initially be made by MN.IT on behalf of the agency-based office, but accounted for against the Agency's (non MN.IT) chart of accounts and funding.

As decisions are made on new projects or service levels throughout the year, the Agency-based CIO will work with the Agency to evaluate the costs associated with those changes, and the implications the changes will have on the Agency's budget. When budget changes are made, this SLA will be modified. See Section 1 for IT budget changes ("Acceptance, Amendments, and Termination"). A more detailed budget/SLA change process is being developed and will be distributed when it is complete.

MNsure Service Costing Details

FY15 Planned IT Spend by Account Class

The following table provides the specific IT service costing for your agency as well as the estimated cost of centrally provided IT services. The IT costs include IT spend by all funds including federal, general and special revenue funds. For Group B agencies, billed only on non-payroll transactions, the budget does not include payroll dollars. These IT costs are shown on an accrual basis. Below the FY15 Accrual Budget by Agency, we have a reconciliation between the cash budget in SWIFT and the accrual budget. The Total Agency IT Budget includes on-going IT projects, Biennial IT (BIT) projects, and Odyssey Fund projects for the FY14/15 biennium.

FY15 Budget - MN.IT @ Agency

Account Class	Account Class Description	FY15 Budget
41000	Full-Time Salary & Fringe*	0
41030	Part-Time Salary & Fringe	0
41050	OT & Premium Pay	0
41070	Other Employee Costs	0
	Total Personnel	**0**
41110	Printing and Advertising	0
41130	Prof/Tech Services Outside Vendor	5,316,400
41145	IT Prof/Tech Services O/S Vendor	0
41150	Computer & Systems Services	0
41155	Communications	0
41160	Travel & Subsistence - In State	0
41170	Travel & Subsistence - Out State	0
41180	Employee Development	0
41190	Agency Provided Prof/Tech Serv	0
41195	IT State Agency Prof/Tech Serv	0
41300	Supplies	306,417
41400	Equipment-Capital Lease	63,500

Account Class	Account Class Description	FY15 Budget
41500	Repairs, Alterations & Maintenance	0
42000	Agency Indirect Costs	0
42010	Statewide Indirect Costs	0
42020	Attorney General Costs	0
42030	State Agency Reimbursements	
42040	Agency Direct Costs	0
43000	Other Operating Costs	8,361,911
44100	Payments to Individuals-Med-Rehab Client	0
44110	Payments to Individuals-Not Med Rehab	0
47040	Intangible-Capital	0
47060	Equipment-Capital	0
47160	Equipment-Non-Capital	0
47010	Building-Improvement-Capital	0
44130	Aid-Grants to Counties	0
44140	Aid-Grants to School Districts	0
44155	Aid-Grants to State Agencies	0
44200	Distrib of Amounts Collected	0
49000	Non-Cash Transactions	0
	Total Non-Personnel	**14,048,228**
	Total Agency-Based IT Budget	**14,048,228**
	Centrally Provided IT Services	**1,713,956**
	Sub-Total Agency IT Budget	**15,762,184**
	Total BIT	**0**
	Total Odyssey Fund	**0**
	Total Agency IT Budget	**15,762,184**

Items Not Included in IT Budget

Account Class	Account Class Description	FY15 Budget
41100	Space Rental, Utilities, & Maintenance	0

Reconciliation of Cash Budget to Accrual Budget

Detail	Spend
Cash Balance	0
+ / - Adjustments	
Accruals - Capitalized Equipment Credit	0
Accruals - Software Amortization	0
Accruals - Depreciation / Interest	0
Accruals - Prepaid Adjustments (Software, Communications, Repairs & Maintenance)	0
Accrual Balance	0

Budget Change Details

The line tiems below represent budget changes to account classes in the FY15 Planned IT Spend by Account Class Table.
Increase = Positive Number
Decrease = Negative Number

Detail	Amount	Detail	Amount

BIT, Odyssey Fund Details

The line items below provide detail for the Total Bit and Total Odyssey Fund line items in both tables.

Detail	Total	Detail	Total

FY15 Budgeted Service Costs, June 2014

The following chart shows the services costs calculated in the MPWR Cost Model for FY15 based on budged volumes and rates.

Group A (Rates) - For those agencies that will be billed based on service rates, the chart below provides the budget-based view where budgeted volumes times budgeted rates = budgeted service cost. Actual volume variances may cause the actual service cost to vary. MN.IT will have a true-up process in place to determine the variance between budgeted service costs and actual service costs.

Group A (Direct Charge) - For those agencies that will be billed for payroll and non-payroll costs based on MN.IT procurement transactions, the chart below is a "showback" to indicate what the budgeted service cost view looks like.

Group B - For those agencies that will be billed for non-payroll costs only based on MN.IT procurement transactions, the chart below is a "showback" to indicate what the budgeted service cost view looks like.

The total amount of enterprise (centrally provided) IT services, BIT and Odyssey Funds are shown as single line items in order to arrive at a total agency IT Spend:

Service Type		FY15 Budget Service Costs
Standard IT Services		0
Client Computing	0	
Enterprise Unified Communication & Collaboration	0	
Contracted Telecom Service	0	
IP Services	0	
Contact Center MN (CCM)	0	
LAN Services - Facilities	0	
WAN/MAN Services - Facilities	0	
Service Desk	0	
Applications		0
Projects and Initiatives		0
Sub-Total Agency-Based Budget Service Costs		**0**
Enterprise (Centrally Provided IT Services)		1,713,956
Total BIT Costs		0
Total Odyssey Fund Costs		0
Total Agency IT Budget Costs		**1,713,956**

Section 7: Information Security

Information Security

Statutory Responsibilities for IT Security

The State of Minnesota recognizes that information is a critical asset. How information is managed, controlled, and protected has a significant impact on the delivery of state services and is vital to maintaining the trust of those that provide data to the State and/or use state programs. Information assets held in trust by the State must be protected from unauthorized disclosure, theft, loss, destruction, and alteration. Information assets must be available when needed, particularly during emergencies and times of crisis.

It is for this reason that Minnesota Statutes, Chapter 16E requires the State Chief Information Officer (State CIO) to define cyber security policies, standards, and guidelines for the executive branch. It is also why those policies are required to be embedded in all executive branch services, systems and processes. Minnesota Statute also gives State CIO authority to install and administer security systems for use by all.

Protecting our digital infrastructure at a reasonable level of risk is the goal. Presently, the State faces a high level of risk due to an inadequate historical investment in security tools, people and processes. At its current funding level, the State's investment in security stands at 2 percent of its total IT budget, compared to an industry standard of 5.4 percent – 6.2 percent. Current levels of security within state agencies are inconsistent and, in some cases, inadequate.

Consolidation of IT services will significantly improve the security profile of the State and make the achievement of an appropriate level of risk more affordable. As consolidation of IT continues and a thorough evaluation takes place, more accurate analysis of individual agency security levels will be available. Long term, however, the executive branch will need to invest more in information security to ensure that key security services and risk levels are standard and acceptable across all agencies, regardless of size and resources.

Enterprise Security Program Framework

MN.IT Services' Enterprise Security Program exists to set the policies and standards that will protect executive branch information assets and ensure compliance with all state and federal regulatory requirements. The Enterprise Security Program uses the 800 series of publications by the National Institute of Standards and Technology's (NIST) as a framework. The NIST 800 series has been adapted to accommodate the unique model of Minnesota's government.
The information security program is divided into four components that contain high-level policies and a series of implementing standards. These policies are located on the MN.IT Services website at http://mn.gov/oet/programs/policies/security/

Enterprise Security Governance

In order to implement the Enterprise Security Program, the State CIO delegates all security-related responsibilities to the State Chief Information Security Officer.

The IT Governance Framework (June 2012) outlines the process for making decisions that impact the risk posture of the executive branch. New policies and standards are reviewed and approved using the processes in the IT Governance Framework. Periodic review of all existing policies and standards will be conducted at least once every two years through the processes described within the framework.

Role of Agency-based CIO

It is the role of MN.IT Services Agency-based CIO to ensure that all Agency security requirements are identified to the State Chief Information Security Officer, incorporated in Enterprise Security Program policies and standards, or met in delivering IT services and managing IT facilities, systems and applications within the Agency.

It is also the responsibility of the Agency-based CIO to manage Agency-based systems and services to an acceptable level of risk as determined in consultation with the business leadership, and in accordance with applicable state and federal policies and regulations. This may include policies and standards that have not yet been addressed by the Enterprise Security Program and/or policies more stringent than those outlined by the Enterprise Security Program. Agency-based CIOs will ensure that mitigating controls are in place to reduce risk to a level that Agency business leadership is willing to accept.

Role of Business

It is the responsibility of Agency business leadership to understand and accept risk, in consultation with MN.IT Services Agency-based CIO, for the services and applications in its portfolio. It also is the responsibility of Agency business leadership to ensure that at least the minimum state policy requirements for security can and will be met at the Agency level.

Through defined governance processes, Agency business leadership has an opportunity to participate in the design and implementation of the policies, standards, and security systems that are required for the executive branch.

Role of MN.IT IT Standards and Risk Management Division

The MN.IT Services IT Standards and Risk Management Division is responsible for the management of enterprise security governance, for monitoring and enforcing compliance with executive branch policies and for the strategic and tactical planning of the Enterprise Security Program. The division is also responsible for planning and/or approving appropriate security services for all executive branch entities. These security services include both Standard IT Services, which are directly used by agencies and Enabling IT Services, which are incorporated within other services and not necessarily visible or “consumable” by the customer. Table 7-1 describes all the information security services provided by MN.IT and outlines whether each service is a Standard IT Service (described further in section 3) or an Enabling IT Service.

The table also outlines the delivery method for each service. To leverage the state's economy of scale, many security services will now be delivered through a primarily centralized model. The remaining security services, which require detailed knowledge of agency business practices, will be rendered by one of six teams that have been formed to deliver services to all of the agencies within the following distinct lines of business:

- Health (23 entities)
- Safety (10 entities)
- Environment (7 entities)
- General Government (10 entities)
- Economic (12 entities)
- Education (11 entities)

The successful delivery of every information security service will necessitate a high degree of coordination and interaction between Central and LOB teams. No information security service can be delivered entirely by either group.

Table 7-1
Types of Information Security Services Provided by MN.IT Services

Security Service	Service Description	Service Delivery Method	Service Type
Governance, Risk and Compliance Services			
Information Security Program Management	Responsible for the planning, oversight, and coordination of all information security activities, including the development of enterprise-wide policies and standards	Primarily Centralized	Standard
Secure System Engineering	Responsible for designing appropriate security controls in new systems or systems that are undergoing substantial redesign, including both in-house and outsourced solutions	Central Direction/Hybrid Delivery	Enabling
Information Security Training and Awareness	Responsible for providing employees at all levels with relevant security information and training to lessen the number of security incidents	Central Direction/Hybrid Delivery	Standard
IT Service Continuity	Responsible for ensuring that critical technology will be available in a time of crisis	Central Direction/Hybrid Delivery	Enabling
Information Security Compliance	Responsible for validating that information security controls are functioning as intended	Central Direction/Hybrid Delivery	Enabling

Operational Security Services			
Information Security Monitoring	Responsible for gaining situational awareness through continuous monitoring of networks and other IT assets for signs of attack, anomalies, and inappropriate activities	Primarily Centralized	Enabling
Information Security Incident Response and Forensics	Responsible for determining the cause, scope, and impact of incidents to stop unwanted activity, limit damage, and prevent recurrence	Primarily Centralized	Standard
Vulnerability and Threat Management	Responsible for continuously identifying and remediating vulnerabilities before they can be exploited	Primarily Centralized	Enabling
Boundary Defense	Responsible for separating and controlling access to different networks with different threat levels and sets of users to reduce the number of successful attacks	Primarily Centralized	Enabling
Endpoint Defense	Responsible for protecting information on computers that routinely interact with untrusted devices on the internet or may be prone to loss or theft	Primarily Centralized	Enabling
Identity and Access Management	Responsible for managing the identities of users and devices and controlling access to resources and data based on a need to know	Central Direction/Hybrid Delivery	Standard
Physical Security	Responsible for protecting information systems and data from physical threats	Central Direction/Hybrid Delivery	Enabling

Section 8: Force Majeure and Performance Exceptions

Force Majeure & Performance Exceptions

Neither party shall be responsible, or considered in default in the performance of its obligations, for failure or delay of performance, including failure to satisfy service availability levels/objectives, if caused by: (1) scheduled downtime to perform routine, non-emergency or emergency maintenance on MN.IT-provided services; (2) downtime on non-production systems; (3) factors outside of the party's reasonable control, including any force majeure event as defined below; (4) equipment, software or other technology not within MN.IT's direct control; (5) service suspensions or termination of Agency's right to use the MN.IT-provided services in accordance with the Agreement.

Force majeure events include, but are not limited to, acts of God, acts of government, flood, fire, earthquakes, civil unrest or riot, acts of terror, acts of war, acts of hostility or sabotage, strikes or other labor problems including a government shutdown, Internet/telecommunications service provider or power/electrical failures or delays, and other events outside the reasonable control of the obligated party.

Both parties will use reasonable efforts to mitigate the effect of a force majeure event. This section does not excuse either party's obligation to take reasonable steps to follow its normal disaster recovery procedures or Agency's obligation to pay for programs delivered or services provided.

Appendix A: Related Information

Related Information

Covered Entities

This SLA describes services provided to the following entity(ies): MNsure

Standard Documentation

The following documents provide additional information regarding MN.IT Services:

- Minnesota Statutes chapter 16E Office of MN.IT Services https://www.revisor.mn.gov/revisor/pages/statute/statute_chapter_toc.php?chapter=16E
- Enterprise Technology Fund 5500 Rate Schedule 2014
- State of Minnesota IT Master Plan, http://mn.gov/oet/about-mnit/strategic-plans.jsp
- Operational documents/information on the MN.IT website http://mn.gov/oet/index.jsp
- Minnesota IT Governance Framework available on the MN.IT website http://mn.gov/oet/about-mnit/governance.jsp

Agency Specific Documentation

The following documents provide additional information specific to MNsure operations:

Document Name: Not available at this time.

Link:

MNsure is a Minnesota state agency established by Minnesota Statutes, chapter 62V as a state health benefit exchange as described in section 1311 of the federal Patient Protection and Affordable Care Act, Public Law 111-148 ("ACA"), and further defined through amendments to the ACA and regulations issued under the ACA. The following clarifications are in addition to the SLA between MNsure and the Office of MN.IT Services ("MN.IT") and are hereby attached to and incorporated into the SLA. To the extent that provisions of the SLA are in conflict with this Appendix A, the terms of this Appendix control.

Since MNsure's creation, MNsure and MN.IT have worked collaboratively to implement the MNsure Health Care Exchange IT project and systems. The relationship is collaborative in nature and includes a robust governance structure; MNsure, the Department of Human Services ("DHS") and MN.IT together created a shared governance structure to oversee the MNsure project.

State statutory exemptions included in chapter 16E

MNsure is considered a state agency pursuant to Minnesota Statutes chapter 16E and is therefore subject to chapter 16E's requirements. However, pursuant to Minnesota Statutes, section 62V.03, subdivision (g), MNsure is statutorily exempt from the following sections of chapter 16E: 16E.01, subdivision 3, paragraph (b); 16E.03, subdivisions 3 and 4; 16E.04, subdivision 1, subdivision 2, paragraph (c), and subdivision 3, paragraph (b); 16E.0465; 16E.055; 16E.145; 16E.15; 16E.16; 16E.17; 16E.18; and 16E.22.

Each statutory exemption is outlined below to ensure a continued and shared understanding of MNsure's unique authority as part of the statewide IT consolidation. The exemptions are outlined with the understanding that both parties intend to continue working collaboratively to ensure best value for the state. However, for the avoidance of doubt, both parties also agree that MNsure's choice to follow MN.IT policies and practices it would otherwise be exempt from does not waive that exemption generally and MNsure may choose to rely upon the exemptions as outlined in law as needed.

Chapter 16E exemptions:

- **16E.01, subdivision 3, paragraph (b);** MNsure is exempt from MN.IT determinations which require state agencies generally to use shared information and telecommunications systems and services, reimbursement rates or billings referenced in paragraph b. Therefore, if it is determined by MNsure governance that shared information and telecommunications technology systems and services for the delivery of electronic government services are unable to meet the needs of MNsure, the MN.IT CIO may not require MNsure's use, nor establish reimbursement rates as further outlined in this section.
- **16E.03, subdivision 3**; MNsure is exempt from written approval by the MN.IT CIO for an information and telecommunications technology project which may be undertaken by MNsure. Therefore, no unencumbered balances of any appropriation allotted for a project may be cancelled by any entity other than MNsure.
- **16E.03, subdivision 4**; MNsure is exempt from the evaluation procedures as described in this section.

- **16E.04, subdivision 1;** MNsure is exempt from MN.IT policies and their enforcement related to the development and purchase of information and telecommunications technology systems, services and training appropriate persons in their use.
- **16E.04, subdivision 2, paragraph (c);** MNsure is exempt from MN.IT approval on requests for grant funding with an information and technology component. MNsure is committed to continued work with MN.IT on any and all grant applications and proposals of this nature moving forward, but MN.IT approval is not required prior to a request for grant funding being submitted.
- **16E.04, subdivision 3, paragraph (b);** MNsure is exempt from the requirement that all applicable risk assessment and mitigation plans be reported to and approved by the chief information officer prior to more than 10% of the proposed budget being spent on the project.
- **16E.0465**; MNsure's appropriation of state or federal funds is not required to divide all technology projects into phases, and is exempt from MN.IT review and affirmative determinations that the project satisfies statutory requirements.
- **16E.055**; MNsure is exempt from the requirement to use the single entry site created by MN.IT for all agencies to use for electronic government services.
- **16E.145**; MNsure is exempt from the requirement that all appropriations for state agency information and telecommunications technology projects be made to the MN.IT CIO.
- **16E.15**; MN.IT is not authorized to sell or license computer software products or services developed by MNsure, or custom developed by a vendor on behalf of MNsure without MNsure's written approval.
- **16E.16**; MNsure is exempt from MN.IT's general statutory authority to require a state agency to adjust its operating management procedures as described and under the circumstance included in this section.
- **16E.17**; MNsure is exempt from MN.IT supervision and control related to MNsure telecommunication facilities and services.
- **16E.18**; MNsure is exempt from these statutory requirements generally as described within this section. Therefore, MNsure reserves the ability to perform the duties outlined within this section and may perform the following duties otherwise reserved for the MN.IT CIO:
    - arrange for IT and telecommunications services
    - manage vendor relationships, network function and capacity planning
    - set rates and fees for services
    - approve contracts for services, facilities or equipment relating to the system
    - develop a system plan and annual program and fiscal plans for system
- **16E.22;** MNsure is exempt from the requirements included in the Statewide Electronic Licensing System.

Interagency Agreement with the Minnesota Department of Human Services

Pursuant to Minnesota Statutes, section 62V.05, subdivision 7, MNsure is required to establish and maintain an agreement with DHS as the designated state Medicaid agency responsible for administering the State's Medicaid Program, a/k/a Medical Assistance ("MA") program, including MinnesotaCare ("MCRE") for cost allocation and services regarding eligibility determinations and enrollment for public health care programs using a modified adjusted gross income standard to determine program eligibility. In addition, MNsure is provided the discretion to establish and maintain an agreement with DHS for additional, other services.

MNsure and DHS have entered into interagency agreements pursuant to Minnesota Statutes, section 471.59, subdivision 10, as needed to facilitate the development, implementation, maintenance, and oversight responsibilities of the Minnesota health care exchange. Additional services MNsure has secured through interagency agreements with DHS include centralized and administrative tasks (i.e. Information Technology support services, accounts payable, purchasing and procurement, Human Resources).

Agency-based Chief Information Officer

Throughout the SLA, the "agency-based Chief Information Officer (CIO)" is referred to as having various and significant roles regarding the relationship between MNsure and MN.IT. Given that MNsure and DHS have chosen to enter into an interagency agreement that allows for joint development, maintenance, and operation of certain IT applications, and for use of certain IT support services, MNsure and MN.IT agree that DHS's agency-based CIO shall also serve as MNsure's agency-based CIO. However, both parties agree that MNsure reserves the right to request that a separate agency-based CIO be appointed and that MN.IT will proceed with such a request subject to appropriate input from MNsure.

Federal Compliance

The parties agree that all final decision making authority resides with MNsure regarding how ACA statutes, rules and publications are to be interpreted for purposes of development, implementation, maintenance, and oversight responsibilities of the state health benefit exchange unless otherwise delegated to another party.

In Witness Whereof, the undersigned government entities have caused the Service Level Agreement and all it appendices to be executed by duly authorized officers.

1. The Office of MN.IT Services

By: _____
(With delegated authority)

Title: _____

Date: _____

2. MNsure

By: _____
(With delegated authority)

Title: _____

Date: _____

Appendix B: Definitions

Definitions

SLA Glossary of Terms

Account Manager: Person assigned to each Agency as a central point of contact from the customer service team

Account Team: Customer service team assigned to each Agency

Agency: Executive Branch Business

Agency Business Division: Primary unit within the agency structure that uses the application

Agency-based Chief Information Officer: The chief information officer located at each agency. For purposes of the Service Level Agreement, the Agency-based CIO also means the Designated IT Lead. The Designated IT Lead means the person assigned to represent MN.IT Services at the agency in lieu of a chief information officer, and may be an employee of another agency.

Agency Applications: Applications and IT services provided by an Agency in support of their customers and business

Agency Threshold: A service threshold that is specific to an Agency, and is different than the documented Standard Threshold

Application Name: How agency staff commonly refer to the application

Attended Hours of Operation: Times when the application should be available for use

Centers of Excellence: A collection of services that is recognized as the lead service provider and available for all executive level agency usage

Change Windows: Scheduled times when IT services may be unavailable while planned changes are being implemented

Cost Model: An financial review of an Agencies IT budget showing Applications, Projects and IT Services

Critical Success Factors: A metric that reports on how effective a particular service is operating

Criticality: Impact if the application becomes unavailable because of an unplanned service incident.

Critical-1 Procedures: Highest level incident/outage, which will follow a specific set of instructions to restore the service and manage communications

Downtime refers to periods when a system is unavailable. Downtime or outage duration refers to a period of time that a system fails to provide or perform its primary function.

Downtime Period is a period of ten consecutive minutes of Downtime. Intermittent Downtime for a period of less than ten minutes will not be counted towards any Downtime Periods.

Emergency change is typically to resolve an ongoing service outage or degradation or address an emerging security vulnerability, in which case the risks and potential business impact are so high that it is not prudent to wait for the next regularly scheduled change window.

Emergency Maintenance: A change window requested for unplanned maintenance to correct a system outage

Enabling IT Services: IT Services provided by MN.IT that are in support of the Business Standard Services. Examples would be Hosting, Storage, Networking, and Data Center Facilities

Incident: An incident is any event which is not part of the standard operation of service and which causes, or may cause, an interruption or a reduction in the quality of that IT service.

IT Consolidation Act: Legislation passed in the 2011 Special Session that consolidated IT from the Executive Branch State Agencies into one organization. Laws of Minnesota 2011, First Special Session chapter 10, article 4.

Management Control Policies: These policies are in place to address RISK throughout the lifecycle of the State's information assets

Metric: A key measure used to communicate how a service is being delivered

Metric Definition: The working definition of a metric

Office of MN.IT Services: Executive branch Agency responsible for delivering IT to all Executive Branch State Agencies

Operational Control Policies: Defines a class of security controls implemented and executed by individuals

Outage when a service is interrupted.

Prioritization: As part of the Incident Management and Service Request Process, each ticket will be classified and assigned a Priority according to its expected Service Level, as well as the number of people being impacted. This will help establish its place in the work and service request queues.

Program Policy: Identifies the overall purpose, scope and governance requirements of a program as a whole

Projects and Initiatives: A list of approved efforts to develop new applications and make changes to existing applications and services

Recovery Time Objective (RTO): The maximum period of time available for recovering an application before there is a significant impact on the agency.

Scheduled Downtime means those times where MN.IT Services notifies agencies of periods of Downtime for Scheduled Maintenance at least five days prior to the commencement of such Downtime.

Scheduled Maintenance: Regular scheduled times for MN.IT staff to perform maintenance to applications and services

Service Availability: The amount of time an application is 'up' during its required availability hours. This is reported as a percentage, e.g. 99.5% or 99.9%. To calculate the service availability:

$$\frac{\text{Required monthly minutes of availability} - \text{minutes of monthly outage}}{\text{Required monthly minutes of availability}} \times 100$$

- **Required monthly minutes of availability** =

  # of days in month application is required x hours required each day x 60 minutes
- **Minutes of monthly outage** = Average historical monthly downtime of application (not including planned maintenance)

Example: Application X has an availability requirement from business of 9 hours a day/5 days a week and has a historical average of 30 minutes of downtime per month. To calculate its service availability:

Required monthly minutes of availability: 22 days x 9 hrs x 60 min = 11,880 min

Minutes of monthly outage = 30

(11,880 – 30)/11,880 x 100 = ***99.7%***

Service Costs: The cost associated with the delivery and support of a specific MN.IT service offering

Service Desk Activity: The work associated managing End User requests and incidents

Service Level Agreement: The documented agreement for delivery and support of MN.IT services between the Executive Agencies and the MN.IT staff

Service Level Objectives: The documented expectation measuring the actual delivery of a service

Service Levels: Measurements detailing the expected delivery of a service

Service Metrics: Specific measures established for each Service being delivered

Service Performance Reports: Regularly published reports depicting actual Service Results using identified metrics

Service Request: A user request for support, delivery, information, advice, documentation, or a standard change. Service requests are not service disruptions.

Services: A list of common tasks and activities performed by MN.IT in support of the Agency employees

Standard IT Services: Business facing services, typically available to all State of Minnesota employees, with approval. Examples are: Order new laptop, Request Access to an Application, Utilize Web Conferencing

Standard Threshold: The established Service Threshold (metric) available for a given Service offering

Support Hours and Availability: Published days of the week and hours of the day when a particular application or service is available for use, and for which support is readily available

Sustaining Documentation: A set of 4 documents which defines the foundation for the directions of the State's IT program. They include:

1. The comprehensive IT Service Level Agreement (this document)
2. The State of Minnesota Information and Telecommunications Systems and Services Master Plan
3. The Agency Centralized IT Reference Model
4. The State of Minnesota IT Governance Framework

Technical Control Policies: Defines a class of security controls executed or used by systems

Uptime is the time period during which the Service Element at the Agency endpoint and the shared infrastructure is fully functional.

Service Support Tiers

Incident Management Quick Reference

Priority

Priority	Description	Resolution Target	Notification/Communication	Media / Timescale
1: Critical	Any Incident that has "massive impact" and is highly visible, impacts a significant number of Users, a major agency, application or service, and has no redundancy or alternate path. Critical-1 Incidents are usually (but not limited to) one of the following issues: ▪ Enterprise e-mail or enterprise messaging outage or impaired service ▪ State portal services down or impaired ▪ VOIP/CCM/phone outage or impaired service ▪ Mainframe or significant LPAR outage or impaired service ▪ Network outage or impaired service impacting large subset of Users	2 Hours (24x7)	1. Incident submission 2. ACD updates 3. Email/phone updates* 4. Incident ticket updates 5. External media (e.g., reporters, newspaper) 6. Incident resolution 7. Incident closure * Email is the preferred medium; phone updates will be utilized as deemed appropriate	1. Automated email 2. Initial; then hourly 3. Initial notification; then hourly 4. Initial acceptance from assignee group within 15 minutes; updates every 30 minutes 5. As determined by the Communication Director and Executive Team 6. Email 7. Automated email

Priority	Description	Resolution Target	Notification/Communication	Media / Timescale
2: High	A priority of High will be assigned to any 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.	8 Hours (24x7)	1. Incident submission 2. Incident ticket updates 3. Email / Phone updates to submitter 4. Incident closure	1. Automated email 2. Initial acceptance from assignee group within 15 minutes; updates every 60 minutes 3. Every two hours 4. Automated email
3: Medium	A priority of Medium will be assigned to any 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.	2 Business Days	1. Incident submission 2. Incident ticket updates 3. Email / Phone updates to submitter 4. Incident closure	1. Automated email 2. Initial acceptance from assignee group within one business hour; updates every 4 business hours 3. Once per business day 4. Automated email
4: Low	Any Incident that impacts: ▪ a small number of Users or a single User, where a resource or non-critical service is down or degraded and a deferred fix or maintenance is acceptable.	5 Business Days	1. Incident submission 2. Incident ticket updates 3. Email / Phone updates to submitter 4. Incident closure	1. Automated email 2. Initial acceptance from assignee group within one business day; updates every two days 3. Minimally twice during lifecycle of Incident 4. Automated email

Incident/Request Status Definitions:

Status	Description
Assigned	The Incident has been assigned to a support group. The Assignee Field is blank. Most tickets/requests are assigned to the Service Desk first. The Service Desk will analyze. Classify, and prioritize the Incident. The Service Desk will either resolve the incident/request or assign to the correct support group.
Accepted	Incident has been accepted by the Support Group and been assigned to an individual in the group to resolve the Incident.
Resolved	The Incident has been fixed with the resolution. The status will change to Resolved with Text in the resolution field and a selection from the menu of Incident/Cause. The Service Desk will confirm the resolution with the customer
Closed	The Service Desk will confirm Incident closure with the customer. Only the Service Desk staff can close Incidents in ARS. Only Incident Manager or Problem Manager can close Critical-1 priority incidents
Suspended Internal	The Incident is being monitored for future occurrences or the incident is awaiting a vendor action. A specific reason must be provided to set an incident to this status. A date/time must be provided for the incident to come out of this status.
Customer Pending	MN.IT is awaiting information from the customer before the Incident/Request ticket can be worked further by MN.IT. You are prompted for a specific and concise explanation of what is needed from the customer in order to set an incident to this status. A date/time must be provided for the incident to come out of this status. An email is sent to the customer with the specific details of what MN.IT needs from the customer in order to proceed

Appendix C: Standard IT Service Descriptions

Standard IT Service Descriptions

The following Standard IT Services have detailed services descriptions on the MN.IT Services website http://mn.gov/oet/services/#

- Connectivity and Mobility
  - Wireless
  - Virtual Private Network (VPN)
  - Cellular Services
- Enterprise Unified Communication & Collaboration
  - EUCC Email, SharePoint (Web Collaboration), Instant Messaging
  - Audio, Video & Net Conferencing
- Facility Services
- Minnesota Geospatial Information Office (MnGeo)
  - Coordination and Professional Services
  - Web Services
  - Geospatial Commons
  - Geospatial Infrastructure Hosting
- Security Services
  - Information Security Program Management
  - Identity and Access Management
  - Security Incident Response and Forensics
  - Information Security Training and Awareness
- Voice Services
  - Dial Tone Services
    - Classic Voice
    - Private Branch Exchange Systems (PBXs)
  - Voice-Related Applications or Services
    - Voicemail
    - Contact/Call Center
    - Interactive Voice Response (IVR)
    - Interpretation
    - e-Fax Services
- Web Management
  - Web Server Management
  - Content Delivery and Migration
  - User Interface Design
  - Information Architecture
  - Accessibility
  - Geospatial Information Office (MnGeo)
- Workstation Management
  - Operating Systems
  - Hardware, Software, Peripherals

Appendix D: Enabling IT Services

Enabling IT Services

Hosting Services: Managed Hosting (Server and Virtualization) Support

Server Build and Installation: Install requested server

Server Operations: Provide 7 x 24 support of servers

Server Maintenance: Perform standard maintenance and patch management

Hosting Services: Managed Hosting (Storage and Backup Support)

Enterprise Storage Services: Provisioning, infrastructure management, maintenance and support

Enterprise Backup Services: Backup policy management, status reporting, infrastructure management, maintenance and support and provide enterprise users with capabilities to recover/restore protected data

Hosting Services: Data Center Management Services

Data Center Operations and Management: Data center physical operations and support

Data Center Operations: Provide 7 x 24 support

Connectivity/Network Services: Network Infrastructure

WAN Management: Provide wide area network services

LAN Management: Provide local area network services

SAN Fabric Services: Provide connection services to storage

Connectivity/Network Services: Boundary Defense

Boundary Defense: Provide security for the networks

Connectivity/Network Services: Directory Services

Active Directory Services: Local active directory services in support of access management

Enterprise Active Directory: Active directory services in support of access management

Domain Name Services: Domain name management

Application & Integration Services: Application Development

Business and Process Analysis: Business process design and analysis

Systems Research and Selection: Review & recommend solutions based on requirements

System Design Application: System design services

System Build Application: System build services

System Testing Application: System testing services

Application Deployment: Deploy approved applications to the environments

MnGeo Development – Geospatial project oversight, data development and strategic planning

Application Development

MnGeo Development: Geospatial project oversight, data development and strategic planning

Application & Integration Services: Application Management

Business application operations and support (COTS): Support commercial software

Application & Integration Services: Database Administration

Database Services: Database design, implementation, maintenance, monitoring, tuning and on-going support

Application & Integration Services: Middleware Administration

Middleware Services: Middleware design, implementation, maintenance, monitoring, tuning and on-going support

Application & Integration Services: Data Management

Records management: Record management services

Information Management: Access to systems information

Reporting and Decision Support: Access to data for reporting and decision support

Business Intelligence: Data analytics in support of the business

Security Services

Secure System Engineering: Design appropriate controls

Information Security Compliance: Validate controls

IT Service Continuity: Technology recovery and planning tools

Information Security Monitoring: Improve situational awareness

Vulnerability and Threat Management: Mitigate known vulnerabilities

Boundary Defense: Firewalls, routers and VPNs

Endpoint Defense: Detect malicious software

Physical Security: Technology and processes

Service Management Services: Service Desk

User Technical Assistance: Day to day technical assistance to users via the Service Desk

Performance Monitoring and Reporting: Monitoring systems performance and stability

Leadership & Supporting Services: IT Supporting Functions

IT Management: Day to day IT management of services

Strategic Planning: Forward looking strategic planning

Portfolio, Program and Project Management: PMO Services

Financial and Staff Management: Provide financial analysis and support

Governance and Customer Relationship Management: Liaison between IT and Agency Customers

Procurement, Deployment and Decommissioning: Manage purchasing requests

Enterprise Architecture: Structure and Operation Definition

Detailed service descriptions are available upon request.