NORTH Dakota | Information Technology
Be Legendary.™

Enterprise Service Level Agreement

Sept. 2023

This document outlines the general characteristics that are applicable to all of North Dakota's enterprise IT services. It acts as a "Service Level Agreement" between the ND Information Technology Department and all customers that utilize enterprise IT services.

Contents

Our "Customer-Centric" Commitment

With the world literally at our fingertips and technology changing at a rate that far exceeds the past, our customers and citizens demand technology to meet the needs of our citizens and business units. Today's customer wants faster response, more agility, and more accessible service that drive business value into the organization.

As the bar is raised with ever evolving technology, North Dakota's Information Technology Department (NDIT) must respond to both the simplest requests and most complicated projects with resolve. NDIT has elevated many IT service platforms and standards, and we are dedicated to our "customer-centric" approach to service.

Customer-centric means customers are the heart of our business; *our goal is to build long- term partnerships and IT solutions*. Customer-centric means we go beyond handling calls effectively. It means the customer is the focal point of all decisions related to delivery products, services and experiences to create customer satisfaction, loyalty and advocacy.

We are empowering employees to better understand our customer's business, take personal accountability for our customer's issues, explain solutions in an understandable manner, and be innovative in addressing the unique business needs of each customer.

Purpose

Service Level Agreements are designed to manage and improve upon the established levels of service between IT providers and customers. The process encourages both parties to realize that they have a joint responsibility for the service. Typically, this generates:

- An understanding of the customer's business processes and drivers
- An acceptance of the benefits of early discussions regarding future changes to service
- Constructive discussions on better ways of meeting the customer's needs

Standards and Guidelines

NDIT will adhere to the Standards and Guidelines developed under North Dakota's Enterprise Architecture (EA) program. North Dakota Century Code (Chapter 54-59) further describes NDIT's obligations under state law.

Data Integrity and Ownership

NDIT will respect the confidentiality of customer data. Employees have undergone criminal background checks, have fingerprints registered with the FBI, and have annually signed an Acknowledgment of Secrecy Provision accepting criminal consequences for inappropriate disclosure of information. NDIT employees in mandatory quarterly cyber security training.

All data in a customer's application belongs exclusively to that customer. If this agreement is terminated, customers may have the option to take their data with them. Costs for the migration of data will be negotiated on a case-by-case basis.

No entity may access the data without a written agreement signed by the authorized representative of the customer. NDIT reserves the right to reference data as part of normal problem-solving methodologies. Specific Federal Tax Information (FTI) Requirements are outlined in Appendix A. Specific HIPAA Privacy Rules regarding Protected Health Information (PHI) and Confidentiality of Alcohol and Drug Abuse Patient Records are outlined in separate Business Associate Agreements.

Security

NDIT will manage and administer access to hosted operating systems, networks, software, and data. NDIT's hosted environment, including databases and applications, is protected by firewalls and is monitored with intrusion detection technologies.

Due to shared infrastructure and change management concerns, customers will not typically be granted administrative access to systems. To aid in troubleshooting and to provide proof of access permissions, NDIT will comply with the Enterprise Architecture Auditing Standard.

In order to communicate any security vulnerabilities or incidents to the necessary individuals, NDIT and its customer shall comply with the Enterprise Architecture Incident, Prevention, Response, and Notification Standard.

Audit and Compliance

Audits provide an independent assessment of NDIT's security policies and practices. NDIT leverages the findings and recommendations from audits to strengthen the security posture for state computing resources and data.

Under the direction of the ND Legislature, the ND Office of the State Auditor contracts biennially with an outside consultant to conduct vulnerability testing of the state's IT infrastructure. During the alternating year, NDIT participates in a SOC2 audit that is scheduled and conducted by the ND Office of the State Auditor. Customers may request and fund additional application audits through joint development and agreement with NDIT and the ND Office of the State Auditor. Upon request, NDIT will provide customers with access to all locations, facilities, sites, and assets needed to conduct audits, investigations, and compliance reviews.

State Audit Reports are published by the ND Office of the State Auditor. Detailed audit findings will be shared with customers when they relate directly to specific agency applications/infrastructure. North Dakota Century Code (Chapter 54-10-29) further defines the audit of computer systems, including the state auditor's requirement for notifying agencies prior to testing. NDIT will also notify customers in advance of any vulnerability testing specifically directed towards agency applications/infrastructure.

Incident Management and Request Fulfillment

NDIT's Service Desk is the "*Single Point of Contact*" for all incidents, problems, questions, requests, and feedback. The Service Desk can be reached 24/7/365 online at northdakota.service-now.com/serviceportal and via telephone at **(701) 328-4470**.

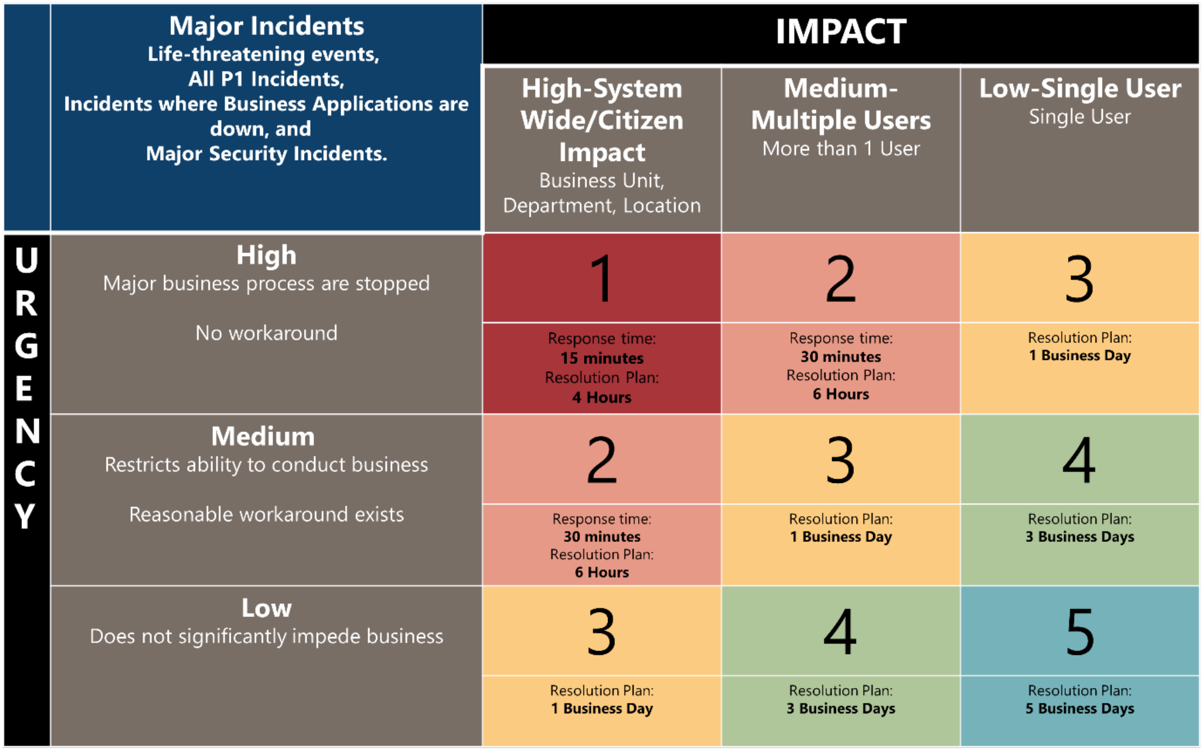
A live analyst will answer calls around-the-clock 24 hours a day and 7 days a week. If an analyst is temporarily unavailable, a response can be expected within 15 minutes.

Incidents

NDIT supports all infrastructure and business applications required to deliver services. NDIT will also assist customers and vendors with troubleshooting. However, customers who do not utilize NDIT's Desktop Support service are ultimately responsible for supporting end-users and desktop computing resources.

If support is required outside of normal business hours with a high priority case (priority 2 or above), customers shall provide NDIT's Service Desk with a list of phone numbers for contacting key business and technical resources within their organization.

Customers may either Submit an Incident Online or call NDIT's Service Desk. All incidents reported to the Service Desk will be assessed a priority based upon the following matrix. NDIT will work with customers to identify the impact that an incident has on their core business and the urgency desired for its resolution.



	Major Incidents Life-threatening events, All P1 Incidents, Incidents where Business Applications are down, and Major Security Incidents.	IMPACT		
		High-System Wide/Citizen Impact Business Unit, Department, Location	Medium-Multiple Users More than 1 User	Low-Single User Single User
URGENCY	High Major business process are stopped No workaround	1 Response time: 15 minutes Resolution Plan: 4 Hours	2 Response time: 30 minutes Resolution Plan: 6 Hours	3 Resolution Plan: 1 Business Day
	Medium Restricts ability to conduct business Reasonable workaround exists	2 Response time: 30 minutes Resolution Plan: 6 Hours	3 Resolution Plan: 1 Business Day	4 Resolution Plan: 3 Business Days
	Low Does not significantly impede business	3 Resolution Plan: 1 Business Day	4 Resolution Plan: 3 Business Days	5 Resolution Plan: 5 Business Days

- Impact reflects the likely effect incidents will have upon core business services.
- Urgency is a measure of the effect on business processes and whether or not primary work functions are able to be performed.
- Together, impact and urgency are blended to determine the priority of an incident.

The priority of an incident will be used to drive NDIT's resource commitment to customers. The estimated resolution times for Incident Management are listed below:

Type	Effort until Resolved/Contained	Response Target	Resolution Target
Priority 1	24/7	15 minutes	4 hours
Priority 2	24/7	30 minutes	6 hours
Priority 3	Business hours		1 day (9 hours)
Priority 4	Business hours		3 days (27 hours)
Priority 5	Business hours		5 days (45 hours)

Service Requests

All service requests are assigned a due date. By default, the estimated due date is set by the Standard Interval defined for the service request type. In all cases, NDIT may negotiate an estimated completion date with the customer in order to accommodate anomalies and additional complexity that exceeds the standard service request type.

The Standard Intervals for Request Fulfillment are listed below:

	Service Request Type	Standard Interval	Responsible Section
1.	Telephone Services • Add • Disconnect	2 business days 5 business days	Technology section
2.	Cellular Devices	7-10 business days	Technology section
3.	Email/Collaboration Tools	2 business days	Technology section
3.	Application Server • New- 3 weeks • Upgrades- 3 weeks • Removals- 2 weeks • Other- varies by request		Technology section
4.	Video Codec Registration	3 business days	Technology section
5.	Server Backup	2 business days	Technology section
6.	Server Monitoring	2 business days	Technology section
7.	Server Restore	2 business days	Technology section
8.	Network Connectivity	5 business days / varies by request	Technology section
9.	Generation Data Group Request	1 business day	Technology section
10.	Database Change Request	5 business days	Technology section
11.	State Forms	5 business days	Records Management
12.	Reverse Proxy	2 business days	Technology section
13.	Mainframe Database Change Request	5 business days	Technology section
14.	Job/Batch Scheduling	3 business days	Technology section
15.	File and Printer Sharing	5 business days	Technology section

	Service Request Type	Standard Interval	Responsible Section
16.	Firewall Request	3 business days	Technology section
17.	ServiceNow Access	3 business days	Technology section
18.	Desktop Support	2-5 business days	Technology section
19.	Generic Service Request	varies by request	Technology section
20.	Remote Access	3 business days	Technology section
21.	Mainframe User ID	3 business days	Technology section
22.	NDGOV User ID	2 business days	Technology section
23.	Peoplesoft User ID	3 business days	Technology section
24.	On-boarding	7 business days	Technology section
25.	Maintain Active Directory Groups	3 business days	Technology section
26.	Initiative Intake	varies by request	Customer Success section
27.	EDMS	5 business days	Technology section
28.	Certificates	1 business day	Technology section
29.	Maintain Charge Codes	3 business days	Finance section
30.	Maintain Department/Division Approver List	3 business days	Technology section
31.	Database ID	5 business days	Technology section
32.	IP Addressing	3 business days	Technology section
33.	DR Testing / Tabletop Exercises	Specific DR test dates are scheduled for each quarter. Submit requests within 90-days of test/exercise.	Security

Customer Satisfaction

Positive feedback encourages people, and constructive criticism improves systems and services. Therefore, customers are emailed an online survey when incidents are resolved or service requests are completed.

The questions can be answered within seconds, and they provide customers with the opportunity to "tell us how we did" in regard to:

- Overall Quality
- Would you contact us again
- Rate your technician
- Courteous and Respectfulness
- Satisfaction

Service Level Objectives

Service Desk:

- 80% of customer calls will be answered within 45 seconds.
- Less than 10% of customer calls will be abandoned after 45+ seconds of waiting.

Incidents:

- 95% of Priority 1 and Priority 2 Incidents will be logged, assigned, and acknowledged/owned by a qualified technician within 15 minutes (Priority 1) and 30 minutes (Priority 2).
- 90% of incidents will be resolved and/or contained by their estimated resolution time.
- 96% of incidents receiving a customer survey response will have a satisfied experience.

Service Requests:

- 80% of service requests will be completed by their standard completion time.
- 96% of service requests receiving a customer survey response will have a have a satisfied experience.

NDIT is committed to managing customer expectations. If the standard interval cannot be met, NDIT's staff will work with the customer to report status and to reassess their expectation for completion.

Major Incidents:

- Is an incident experiencing or affecting an enterprise-wide outage (meaning multiple agencies cannot conduct core business), public safety alerts, or serious political ramifications.

Problem Management:

- It's a cause, or potential cause, of one or more incidents. Problems can be raised in response to a single significant incident or multiple similar incidents.
- The purpose of the problem management practice is to reduce the likelihood and impact of incidents by identifying the actual and potential causes of incidents; and managing workarounds and known errors.
- Our main goal is to find the root cause and provide a fix if one hasn't already been discovered. This can be done two different ways:
  - Reactive – solve problems in response to one or more incidents
  - Proactive – prevent incidents by identifying and solving problems before incidents occur
- Problem records are required when:
  - A major incident has been declared

For more information on Major Incidents and Problem Management refer to the following Knowledge Articles:

- KB1116390-Major Incident
- KB0015844- Problem Management

Change Management

NDIT strives to achieve maximum uptime during normal business hours. All changes will follow NDIT's internal change enablement process, which is based on the ITIL practice for change enablement. The process is available for review upon request and is also available in Knowledge Article KBB0015475.

Scheduled Maintenance

- Unless otherwise pre-approved by customers, scheduled maintenance that causes an interruption in service will be performed during predefined Change Windows:
  - **Network service**: Potentially every Saturday from 4:00 a.m. to 8:00 a.m. Central Time. Higher Education maintenance may also occur on Tuesdays from 4:00 a.m. to 6:00 a.m. Central Time.
  - **Mainframe service**: Potentially every Wednesday morning from 4:00 a.m. to 5:00 a.m. Central Time and the timeframe referenced in the "All other services" shown below.
  - **PowerSchool service**: Potentially any evening from 11:00 p.m. to 5:00 a.m. Central Time and the timeframe referenced in the "All other services" shown below.

  - **All other services**: Potentially every Sunday from 4:00 a.m. to 3:00 p.m. Central Time, but typically limited to the second and/or third Sundays of the month for systems requiring stability at the beginning and/or end of the month.

- Maintenance to test environments will be performed as necessary during normal business hours.
- NDIT will notify customers of scheduled maintenance at least 48-hours in advance.
- Customers may receive Scheduled Change Notifications via email by completing an Online Email Subscription Request.
- Exceptions to the normal maintenance schedule may be granted when special business requirements exist. Customer should make NDIT aware of any unique circumstances.
- Freeze Windows identify time frames when non-emergency change activity is scrutinized and/or postponed. Typically, these windows are influenced by peak business activity, public safety concerns, and/or regulatory demands. *Some examples* of Freeze Windows include:
  - Odd-numbered years from January-April; to accommodate the ND Legislative Session
  - Periods when winter storms are imminent; to accommodate the Dept. of Emergency Services, Highway Patrol, and the Dept. of Transportation
  - The week after the first Monday of November in even-numbered years; to accommodate the Secretary of State's compilation of election results
  - April 1, opening weekend of upland game hunting and the final day for submitting deer gun-hunting applications; to accommodate the Game & Fish Dept.'s online licensing system
  - The first two weeks in April, to accommodate individual income tax return processing by the ND Tax. Dept.

Emergency Maintenance

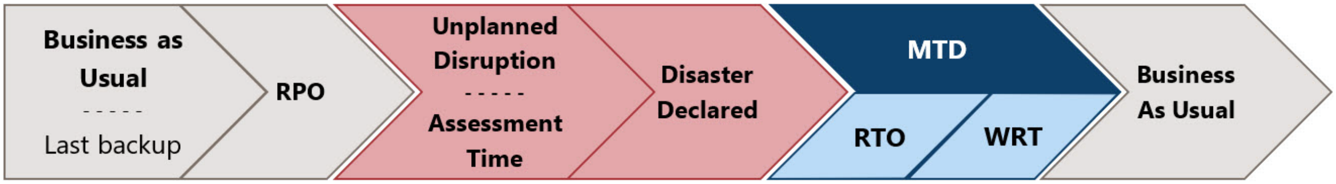
- To address critical situations, NDIT may be required to perform maintenance that disrupts service outside of predefined Change Windows and/or with less than 48-hours notice.
- On occasion, system availability may be interrupted due to conditions outside the direct control of NDIT.
- During times of unscheduled maintenance, NDIT's Service Desk strives to keep customers informed of status updates and estimated completion times.

After changes occur, NDIT's operational processes and monitoring tools will detect the majority of related incidents. However, customers are strongly encouraged to test critical systems prior to normal business hours.

Business Continuity and Disaster Recovery

There are several components to consider when planning for data backup and system recovery are:

1. **Recovery Point Objective (RPO)**
   The point in time to which data can be recovered when a disaster occurs. RPO refers to the last successful data replication or backup. It focuses on data and is independent of the time it takes to get non-functional system components back on-line.
2. **Recovery Time Objective (RTO)**
   A measure of how long it takes for a system to resume operations after a disaster has been declared.
3. **Work Recovery Time (WRT)**
   The amount of time it will take to validate functionality and data availability in the system after recovery plus the time to input any backlogged information.
4. **Maximum Tolerable Downtime (MTD)**
   The total amount of time it takes to recover a system (RTO) plus the time required to validate functionality and data and catch-up on backlogged work accumulated while the system was unavailable (WRT).



NDIT is continually striving to improve its disaster recovery posture within an acceptable rate of investment for its customers. Although steps have been taken to mitigate risks, recovery time objectives and recovery point objectives may be negatively impacted if:

- Enough NDIT personnel are unavailable following a disaster,
- Both the primary and secondary datacenters are seriously impacted by a disaster, or
- The incident involves a cyberattack.

When widespread disasters occur, a variety of IT recovery efforts can be conducted in parallel. However, when competing interests and/or conflicting priorities collide, the following order will be used in determining staff and IT resource allocation:

1. Systems supporting human life and public safety

2. Systems supporting critical human needs (i.e., food, shelter, clothing, and medicine)
3. Systems supporting financial stability
4. All other systems

Declaring a Disaster

To ensure proper escalation and tracking, the following procedure should be used in the event of a disaster. (Agencies should include steps 1-3 in its disaster recovery plans.)

1. A representative from the affected agency will call the NDIT Service Desk to declare a disaster. The person must state that "*this is an emergency notification*" and provide:
   - Agency representative's name.
   - Agency declaring a disaster.
   - A telephone number and other appropriate contact information.
   - A brief description of the incident.
2. The NDIT Service Desk will log an incident, and an NDIT Incident Manager will be designated.
3. The NDIT Incident Manager will contact the original caller and obtain:
   - A more detailed description of the disaster.
   - A determination of whether the agency director and/or IT coordinator has been notified.
   - The location of affected site(s) and any alternate sites.
   - A list of services required from NDIT, including telephone, data network, etc.
4. The NDIT Incident Manager will activate the divisions of NDIT needed for the recovery. At this point, the agency may work directly with those divisions in the recovery.
5. If necessary, the NDIT Incident Manager will contact the agency director and/or its IT coordinators to provide updates.
6. The NDIT Incident Manager will work with NDIT's staff to update the incident log as needed.

Disaster Recovery Testing

NDIT recommends that agencies conduct disaster recovery (DR) tests of their critical hosted systems on a periodic basis. DR testing helps establish if predetermined RTOs can be met; provides feedback to the agency so DR plans can be amended should issues arise; and ensures that the system recovers properly after new upgrades or changes are made to the system.

DR tests are conducted at predetermined times.

- Mainframe DR testing | full week in May (Mon-Fri)
- Once every quarter on predetermined days (Sat or Sun) in March, June, September, and December. The specific dates of these days will be communicated along with other Scheduled Outage and Change Notifications

If extensive testing is required, agencies may be billed at current billing rates for all NDIT staff participating in the exercise.

Tabletop Exercises

NDIT will also facilitate tabletop exercises upon request. A tabletop exercise involves a made-up but possible scenario and then walks through the steps of recovery from both the agency's and NDIT's perspectives.

These exercises are a walk-through of plans for both NDIT and the requesting agency to ensure that both agencies are in accord on the process and expectations of recovery and to identify and remediate any gaps on our processes.

Scheduling a DR Test or Tabletop Exercise

Requests for a DR test or tabletop exercise must be submitted to NDIT at least three (3) months in advance of the requested test/exercise date. DR tests are to be scheduled for the predetermined quarterly test dates.

1. Login to the NDIT ServiceNow Portal
2. Click Request Something
3. Select Governance, Risk, and Compliance from the menu on the left
4. Select Disaster Recovery
5. Complete the form as outlined in ServiceNow; include
    a. Tabletop exercise topic/objective (if known)
    b. Application(s) and server(s) included in the DR test or tabletop exercise
    c. Special instructions
    d. Attach any test scripts, past test reports, or other documents that will help the team prepare
6. Click Submit

Rate Structures

NDIT is primarily funded with Special Funds: Customers pay NDIT for technology services with money allocated in their budgets by the legislature. NDIT generates monthly billings at the beginning of each month for services provided from the previous month. The services are divided onto two separate billings: Data Processing and Telecommunications. Additional information regarding billing, rates, and budget guidelines is available at https://www.ndit.nd.gov/support/billing

Performance Review

SLA performance will be reviewed as needed; at the discretion of NDIT and/or its customers. If it is determined that the conditions of the SLA are not being met, the following will occur:

- NDIT and its customers will openly and constructively discuss the issues.
- Alternatives will be developed, documented, and evaluated.
- All parties will work towards a consensus in selecting the best solution.
- Corrective action will be taken, and progress will be monitored.

NDIT conducts an annual executive level IT Satisfaction survey during the 3rd quarter to assess the previous year. The results are used to:

- Monitor the objectives outlined within NDIT's Strategic Plan.
- Report customer satisfaction indexes to stakeholders.
- Measure the efficiency and effectiveness of services.
- Drive lasting improvements.

NDIT's vision is to be the trusted business partner and preferred IT provider for strategic services. Every effort will be made to accommodate customer concerns. However, if performance problems persist and acceptable solutions are not forthcoming, customers reserve the right to file a formal complaint.

Escalation and Formal Complaints

North Dakota Century Code requires NDIT to document information related to service support and delivery, including agency complaints regarding dependability, responsiveness, and cost.

Customers are encouraged to utilize NDIT's Service Desk as their primary channel for escalating concerns with service support and delivery. However, any of the following individuals may be contacted directly if traditional means of escalation fail to meet expectations:

Point of Contact	Title	Telephone Number

Service Desk	Customer Technical Support Specialists	701-328-4470
Randy Jensen	Enterprise Service Desk Team Lead	701-328-3004
Damon Huck	Tier 2 Team Lead	701-328-3242
Tim Degraff	IT Service Operations Manager	701-328-1940
Kory Hellman	Systems Infrastructure Manager	701-328-1012
Marq Blanks	Network and Facilities Infrastructure Manager	701-328-4472
Hemal Basra	Service Management Director	701-328-4336
Brent Aberle	Could and Infrastructure Director	701-328-3957
Craig Felchle	Chief Technology Officer	701-328-2582

When all other means of communication have been exhausted and expectations remain unfulfilled, customers may submit an incident in the NDIT Self Service Portal. NDIT is required to report upon this information to the Legislative Information Technology Committee and the OMB Budget Section as requested.

Role of the IT Coordinator

For agencies that have been unified, it is understood that the Customer Success Manager/NDIT will be playing a critical role in supporting the needs of the agency and fulfilling these duties.

North Dakota Century Code (Chapter 54-59-10) states "each agency or institution shall appoint an information technology coordinator. The coordinator shall maintain liaison with the department (NDIT) and assist the department (NDIT) in areas related to making the most economical use of information technology."

IT Coordinators are ultimately accountable for a wide-variety of functions. In most agencies, the IT Coordinator will:

- Prepare the agency's IT plan; manage and maintain strategic IT goals and initiatives.
- Manage and maintain the agency's IT budget; forecast requirement and schedule expenditures.
- Organize and execute overall IT functions required to meet business and staff needs.
- Conduct surveys and audits to verify IT effectiveness.
- Implement disaster recovery and backup procedures.
- Implement information security and control procedures.

Agencies need to notify the NDIT Service Desk whenever their primary IT Coordinator changes. Agencies may designate additional people to receive correspondence sent from NDIT to IT Coordinators.

Consent

This agreement will evolve over time as business requirements and technical capabilities evolve. **Ongoing dialog is strongly encouraged.**

Changes to this agreement may be proposed by either party at any time. Any changes proposed may require renegotiating and must be approved by both parties. At a minimum, a review of this

document should be conducted annually. This document remains in effect until it is replaced with an updated version.

North Dakota Information Technology and their stakeholders reviewed and agreed to the terms of this document.

Modifications

Date	SLA Modification
2010-06-04	In Modifications and Consent section, update the agreement date to May 25, 2010
2010-06-04	Added Modifications Pending Mutual Approval section
2010-06-04	In the Performance Review section, "SLA performance will be reviewed regularly" was changed to "SLA performance will be reviewed as needed; at the discretion of NDIT and/or its customers."
2010-06-25	Updated NDIT logo and added "State of North Dakota" / "Information Technology Department" to header
2011-01-07	Redirected hyperlinks/endnotes to content on NDIT's new website
2011-04-06	In Modifications and Consent section, update the agreement date to March 9, 2011
2011-04-06	In Data Integrity and Ownership section, added link to Acknowledgment of Secrecy Provision
2012-08-03	Clarified that scheduled outages may occur on any given Sunday, with special consideration to systems requiring beginning and/or end of month stability.
2012-10-08	Changed the URL for Scheduled Changes
2013-02-05	Changed Standard Interval of Disaster Recovery requests from 1 Day to N/A
2013-02-05	Moved Business Continuity section from Hosting SLA into this document
2013-02-05	Added procedure for Declaring a Disaster

Date	SLA Modification
2013-06-06	Clarified method for subscribing to the Security Officers Listserv
2013-06-06	Added a section for Disaster Recovery Testing
2013-06-12	Changed CIO contact information
2013-11-26	Changed/added CIO and Deputy CIO contact information
2013-12-27	Added Role of the IT Coordinator section
2014-09-16	Added predetermined times for Disaster Recovery testing and added Ryan Huber as a point of contact for escalation
2014-09-29	Added Appendix A regarding Federal Tax Information (FTI) Responsibilities, and changed Consent to come from the IT Coordinators Council instead of the Enterprise Architecture Review Board
2014-12-23	Redirected hyperlinks/endnotes to correspond with URL restructuring of EA standards and removed link to retired NDIT Broadcast System
2015-05-15	Added “NDIT User ID” request with a Standard Interval of 5 Business Days
2015-05-29	Changed “DELA” to “Mainframe” under Disaster Recovery Testing
2015-06-12	Added Audit and Compliance section, incorporating content from Security
2015-10-19	Redirected hyperlinks/endnotes to content on NDIT’s new website and removed Micrographics from Rate Structures
2016-04-25	Minor revisions in Business Continuity section to align with other NDIT Disaster Recovery documentation
2016-05-23	Converted document from PDF to HTML format
2016-09-07	Noted under Data Ownership and Integrity that separate Business Associate Agreements are used to address HIPAA requirements
2017-01-20	Updated personnel listed for Escalation
2018-02-14	Updated customer survey metrics to remove assumptions of satisfaction
2018-11-06	Added opportunities for alignment within Role of the IT Coordinator

Date	SLA Modification
2022-12-21	Updated branding, website links. Updated language in all sections of the document to reflect current practices. The table for Standard Intervals for Request fulfillment was completely updated. Information on Major Incidents and Problems was added.

Appendix A -- Federal Tax Information (FTI) Responsibilities

This appendix outlines specific characteristics associated with information technology services and expands upon the Service Level Agreement between the ND Information Technology Department (NDIT) and the ND state agencies (hereafter referred to as Customer) receiving federal tax information (FTI) from the Internal Revenue Service (IRS). In order to receive FTI from the IRS, Customers must maintain the confidentiality of the FTI and comply with safeguarding requirements of the IRS. NDIT maintains the state's technology infrastructure and hosts certain records on behalf of its Customers. Therefore, the IRS allows FTI to be accessed by NDIT, if NDIT agrees to provide the safeguards outlined in IRS Publication 1075.

I. PERFORMANCE

In performance of this contract, NDIT agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

1. All work will be performed under the supervision of NDIT.
2. NDIT and NDIT's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. NDIT will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
3. FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than NDIT or NDIT's officers or employees authorized is prohibited.
4. FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
5. NDIT will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by NDIT at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, NDIT will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
6. Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, NDIT will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
7. All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements,

the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.

8. No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
9. NDIT will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
10. (To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, NDIT shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward NDIT, and the subcontractor shall assume toward NDIT all the same obligations, duties and responsibilities which NDIT assumes toward the agency under this contract.
11. In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to NDIT hereunder by the same terms and conditions by which NDIT is bound and obligated to the agency under this contract.
12. For purposes of this contract, the term "NDIT" includes any officer or employee of NDIT with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.
13. The agency will have the right to void the contract if NDIT fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

1. Each officer or employee of NDIT to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.
2. Each officer or employee of NDIT to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.
3. Each officer or employee of NDIT to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or

disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

4. Additionally, it is incumbent upon NDIT to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to NDITs by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a NDIT, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
5. Granting NDIT access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A NDIT and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a NDIT and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 (see Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, NDIT and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24-hour notice, shall have the right to send its inspectors into the offices and plants of NDIT to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where NDIT is found to be noncompliant with FTI safeguard requirements.