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 the speed of light, our customers have become more information driven and computer-savvy. Today's customer wants faster, more responsive, more accessible service. To meet their demands, information technology responsiveness must always progress; it is a bar that is constantly elevated.

As the bar is raised, North Dakota's Information Technology Department (ITD) must respond to both the simplest requests and most complicated projects with resolve. ITD 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 we address all customer issues fully and resolve them completely.

We are empowering employees to better understand our customer's business, take personal accountability for our customer's issues, explain solutions in layperson's terms, refer for more technical intervention as needed, 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

ITD will adhere to the Standards and Guidelines developed under North Dakota's Enterprise Architecture (EA) process. The goal of EA is to create a common statewide architecture and to set the future direction of information technology in North Dakota government. EA is a cooperative and collaborative process involving ITD, the Office of Management and Budget, and various state agencies.

North Dakota Century Code (Chapter 54-59) further describes ITD's obligations under state law.

## Data Integrity and Ownership

ITD 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.

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. ITD 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

ITD will manage and administer access to hosted operating systems, networks, software, and data. ITD's hosted environment, including databases and applications, is protected by a firewall and 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, ITD will comply with the Enterprise Architecture Auditing Standard.

In order to communicate any security vulnerabilities or incidents to the necessary individuals, ITD and its customer shall comply with the Enterprise Architecture Incident Prevention,

Response, and Notification Standard. In addition, one or two individuals from each entity should subscribe on-line to the Security Officer's Listserv by sending an enrollment request along with their name, agency name, phone number and e-mail address to itdsecur@nd.gov. Following enrollment and account verification, ITD will inform members of any security vulnerabilities or threats it is aware of within its environment or within the IT community in general. Members may also distribute information to other subscribers by sending to easecurityofficer@nd.gov.

# Audit and Compliance

Audits provide an independent assessment of ITD's security policies and practices. ITD 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, ITD 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 ITD and the ND Office of the State Auditor. Upon request, ITD 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. ITD will also notify customers in advance of any vulnerability testing specifically directed towards agency applications/infrastructure.

# Incident Management and Request Fulfillment

ITD'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 online at www.nd.gov/support and via telephone at **(701) 328-4470** or **(877) 328-4470**.

A live analyst will typically answer calls around-the-clock on weekdays, including Good Friday, Christmas Eve, and any state holiday that falls within a legislative session. On weekends (between Saturday at 8:00 AM and Monday at 7:00 AM Central) and on all other weekday holidays, customers may leave a voice-message for an on-call analyst. A response can be expected within 15 minutes.

## Incidents

ITD supports the infrastructure required to deliver services. ITD will also assist customers and vendors with troubleshooting. However, customers who do not utilize ITD's Desktop

Support service are ultimately responsible for supporting end-users and desktop computing resources.

If support is required outside of normal business hours, customers shall provide ITD's Service Desk with a list of personal phone numbers for contacting key business and technical resources within their organization.

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

**MAJOR INCIDENT**

- Life-threatening events
- Multiple agencies cannot conduct core business
- Serious political ramifications

| URGENCY | IMPACT: HIGH<br>Cannot conduct core business | IMPACT: MEDIUM<br>Restricts ability to conduct business | IMPACT: LOW<br>Does not significantly impede business |
|---|---|---|---|
| HIGH<br>Requires immediate attention | 1 | 2 | 3 |
| MEDIUM<br>Requires resolution in near future | 2 | 3 | 4 |
| LOW<br>Does not require significant urgency | 3 | 4 | 5 |

- Impact reflects the likely effect incidents will have upon core business services.
- Urgency is an assessment of the speed with which an incident requires resolution.
- Together, impact and urgency are blended to determine the priority of an incident.
- A priority of 1-5 is typically assigned, unless the incident is a Quick Fix that can be immediately resolved by ITD's Service Desk.

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

| Type | Effort until Resolved/Contained | Estimated Resolution Within |
|---|---|---|
| Quick Fix | First Call Resolution, 24/7 | 15 minutes |
| Priority 1 | Requires immediate attention, 24/7 | 2 hours |
| Priority 2 | Requires immediate attention, 24/7 | 4 hours |
| Priority 3 | Business hours | 1 day (9 hours) |
| Priority 4 | Business hours | 3 days (27 hours) |
| Priority 5 | Business hours | 1 week (45 hours) |

Business hours are 8:00 a.m. to 5:00 p.m. Central, Monday through Friday; excluding state holidays.

## Service Requests

Customers shall submit all service requests via ITD's Work Management System (WMS). WMS training and guidance is available upon request. Customers shall provide ITD's Service Desk with a list of people that are authorized to submit service requests on their behalf.

All service requests are assigned an estimated completion date. By default, the estimated completion date is based upon either the required completion date specified by the customer or the Standard Interval defined for the service request type – whichever is greater. If a service request type is too broad for Standard Intervals to be applicable, the required completion date specified by the customer becomes the default estimated completion date. In all cases, ITD may negotiate an estimated completion date with customers in order to accommodate for anomalies in resources or complexity.

The Standard Intervals for Request Fulfillment are listed below:

| Service Request Type | Standard Interval | Responsible Section |
|---|---|---|
| Generic | N/A | All |
| General Server | N/A | Distributed Systems |
| WebSphere Deployment | N/A | Distributed Systems |
| EDMS | N/A | EDMS |
| Disaster Recovery | N/A | Security |
| Software Dev/GIS/Proj Mgmt. | N/A | Software Development |
| Batch Generation Data Group | Same Business Day | Computer Operations |
| Batch JCL Maintenance | Same Business Day | Computer Operations |
| Batch On-Demand Report Transfer | Same Business Day | Computer Operations |
| Batch Rerun/Restart | Same Business Day | Computer Operations |
| Batch Special Run | Same Business Day | Computer Operations |
| Database Change | Same Business Day | Database |

| Service Request Type | Standard Interval | Responsible Section |
|---|---|---|
| File/Print Server | Same Business Day | Distributed Systems |
| Email/IM/Fax/Quota | 1 Business Day | Distributed Systems |
| AS400 User ID | 1 Business Day | Security |
| Dataset Authorization | 1 Business Day | Security |
| Dial-Up Access | 1 Business Day | Security |
| FTP Access | 1 Business Day | Security |
| Firewall Access | 1 Business Day | Security |
| ITD User ID | 5 Business Days | Security/Desktop Support |
| LDAP Access | 1 Business Day | Security |
| Mainframe User ID | 1 Business Day | Security |
| Oracle User ID | 1 Business Day | Security |
| Reverse Proxy | 1 Business Day | Security |
| Virtual Private Network (VPN) | 1 Business Day | Security |
| Windows Domain User ID | 1 Business Day | Security |
| Mainframe/AS400 Terminal Printer | 1 Business Day | Service Desk |
| Web Changes | 1 Business Day | Software Development |
| ConnectND User ID | 3 Business Days | Security |
| Storage | 5 Business Days | Storage |
| Network (IP provisioning) | 1 Business Days | Service Desk |
| Network (Disconnect) | 1 Business Day | Telecommunications |
| Network (Port provisioning) | 3 Business Days | Telecommunications |
| Network (New wall jack installation) | 7 Business Days | Telecommunications |
| Network (WAN connection) | 4 Weeks | Telecommunications |
| Network (Other) | N/A | Telecommunications |
| Voice (Disconnect) | 2 Business Days | Telecommunications |
| Voice (Moves, Adds, & Changes) | 5 Business Days | Telecommunications |
| Voice (New wall jack or Smartphone) | 7 Business Days | Telecommunications |
| Voice (Menu or ACD Changes) | 2 Weeks | Telecommunications |
| Voice (Other) | 3 Business Days | Telecommunications |

Business hours are 8:00 a.m. to 5:00 p.m. Central, Monday through Friday; excluding state holidays.

## 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:

- Courtesy and Professionalism
- Skills and Knowledge
- Quality of Work
- Timeliness of Work
- Overall Experience

### Service Level Objectives

**Service Desk:**

- 80% of customer calls will be answered within 20 seconds
- Less than 10% of customer calls will be abandon after 20+ seconds of waiting

**Incidents:**

- 95% of incidents will be logged, assigned, and acknowledged/owned by a subject-matter-expert within 15 minutes of being reported
- 90% of incidents will be resolved and/or contained by their estimated resolution time
- 95% of incidents receiving a customer survey response will have an overall experience rating of “Satisfied” or “Very Satisfied”

**Service Requests:**

- 90% of service requests will be completed by their estimated completion date
- 95% of service requests receiving a customer survey response will have an overall experience rating of “Satisfied” or “Very Satisfied”

ITD is committed to managing customer expectations. If an estimated date cannot be met, ITD’s staff will work with the customer to report status and to reassess their expectation for completion.

## Change Management

ITD strives to achieve maximum uptime during normal business hours. All changes will follow ITD’s internal change management process, which is available for review upon request.

### 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. Higher Education maintenance may also occur on Tuesdays from 4:00 a.m. to 6:00 a.m. Central.
    - All other services: Potentially every Sundays from 6:00 a.m. to 3:00 p.m. Central, 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.
- ITD will notify customers of schedule maintenance at least 48-hours in advance.
- ITD will publish Scheduled Changes online. Customers may also 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 ITD 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, ITD 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 ITD.
- During times of unscheduled maintenance, ITD's Service Desk strives to keep customers informed of status updates and estimated completion times.

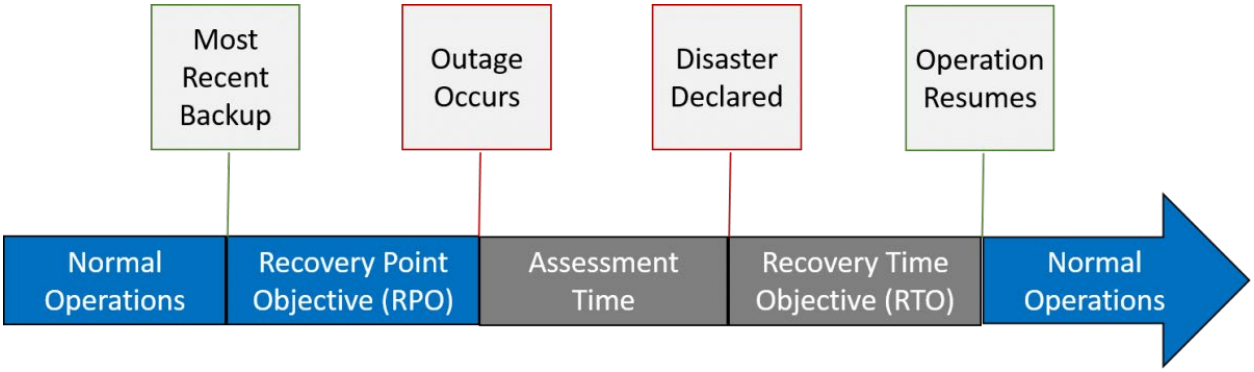
After changes occur, ITD's operational processes and monitoring tools will detect the majority of related incidents. However, customers are strongly encouraged to test critical systems prior to normal business hours.

## Business Continuity

Two 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 time of the last successful data replication or backup. It focuses on data; it 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




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

- A sufficient number of ITD personnel is unavailable following a disaster
- Both the primary and secondary datacenters are seriously impacted by a disaster

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, such as 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 followed in the event of a disaster. (Agencies should include steps 1-3 in their disaster recovery plans as well.)

1. A representative from the affected agency will call the ITD Service Desk to declare a disaster. The person must state that "*this is an emergency notification*" and provide:

- Their name
- Their agency's name
- A telephone number and other appropriate contact information

- A brief description of the incident

2. The ITD Service Desk will log an incident, and an ITD Incident Manager will be designated
3. The ITD 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 ITD, including telephone, data network, etc.

4. The ITD Incident Manager will activate the divisions of ITD needed for the recovery. At this point, the agency may work directly with those divisions in the recovery.

5. If necessary, the ITD Incident Manager will contact the agency director and/or IT coordinators to provide updates.

6. The ITD Incident Manager will work with ITD's staff to update the incident log as needed

Note: Agencies planning to relocate proactively prior to a disaster should submit a Disaster Recovery request via ITD's Work Management System (WMS).

### Disaster Recovery Testing

- Disaster Recovery (DR) tests will be conducted at predetermined times:
    - Mainframe DR testing occurs during a full week in May (Monday – Friday)
    - Other DR testing occurs during three weekends (Saturday – Sunday); one in June, one in October, and one in December
    - Specific dates will be communicated along with other Scheduled Outage and Change Notifications
- Agencies should schedule DR tests at least 3 months in advance by submitting a Disaster Recovery request via ITD's Work Management System (WMS).
- Agencies should provide ITD's architects with a written description of the test scope/expectations at least 2 months prior to the event.
- Agencies will be billed at current billing rates for all ITD staff participating in the exercise.

## Rate Structures

ITD is primarily funded with Special Funds: Customers pay ITD for technology services with money allocated in their budgets by the legislature. ITD 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 www.nd.gov/itd/billing.

# Performance Review

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

- Non-compliance issues will be documented.
- ITD 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.

ITD conducts an annual customer survey in July to assess the previous fiscal year. IT coordinators, business professionals, and agency directors are strongly encouraged to participate. The results are used to:

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

ITD'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 ITD to document information related to service support and delivery, including agency complaints regarding dependability, responsiveness, and cost.

Customers are encouraged to utilize ITD'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 | ITD Service Desk Manager | (701) 328-3004 |
| Tim Degraff | ITD IT Service Manager | (701) 328-1940 |
| Hemal Basra | Director, Service Management | (701) 328-4336 |
| Duane Schell | Chief Technology Officer | (701) 328-4360 |

When all other means of communication have been exhausted and expectations remain unfulfilled, customers may elect to register a Formal Complaint online. ITD 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

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 (ITD) and assist the department (ITD) 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

Key opportunities for aligning IT Coordinators and ITD include:

- IT Directional Meetings: Held 2-3 times a year to recap activities/events, set expectations for what's coming, and spark collaboration/feedback
- IT Coordinators Council Meetings: Held 10-12 times a year to collaborate on enterprise architecture design principles and make recommendations regarding business-related standards/initiatives
- Enterprise Architecture Meetings: Held 8-12 times a year per domain to collaborate on enterprise architecture principles and make recommendations regarding application, data, security, and technology standards/initiatives

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

On February 14, 2018, the Information Technology Department and the IT Coordinators Council (ITCC) agreed to the terms of this document. Additional signatures may be provided as needed.

| Name | Title | Organization | Date |
|---|---|---|---|
| | | | |

# 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 ITD and/or its customers.” |
| 2010-06-25 | Updated ITD logo and added “State of North Dakota” / “Information Technology Department” to header |
| 2011-01-07 | Redirected hyperlinks/endnotes to content on ITD’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 |
| 2013-06-06 | Clarified method for subscribing to the Security Officers Listserv |
| 2013-06-06 | Added a section for Disaster Recovery Testing |

| Date | SLA Modification |
|---|---|
| 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 ITD Broadcast System |
| 2015-05-15 | Added “ITD 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 ITD’s new website and removed Micrographics from Rate Structures |
| 2016-04-25 | Minor revisions in Business Continuity section to align with other ITD 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 |

# 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 (ITD) 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. ITD maintains the state's technology infrastructure and possesses certain records on behalf of its Customers. Therefore, the IRS allows FTI to be accessed by ITD, if ITD agrees to provide the safeguards outlined in IRS Publication 1075.

## Performance

In serving Customers with access to FTI, ITD agrees to comply with and assume responsibility for compliance by its employees with the following requirements:

1. All work will be done under the supervision of ITD.
2. Any return or return information made available in any format shall be used only for the purpose of serving Customers. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in serving Customers. Disclosure to anyone other than an officer or employee of ITD will be prohibited.
3. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
4. ITD certifies that the data processed for Customers will be completely purged from all data storage components of its computer facility, and no output will be retained by ITD at the time the work is completed. If immediate purging of all data storage components is not possible, ITD certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
5. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to Customers or their designee. When this is not possible, ITD will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide Customers or their designee with a statement containing the date of destruction, description of material destroyed, and the method used.
6. All computer systems receiving, processing, storing, or transmitting Federal tax information must meet the requirements defined 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 Federal tax information. Customers and ITD recognize that significant changes to existing architecture, policy, procedures, and processes will be necessary to meet the requirements defined in IRS Publication 1075. ITD is actively working towards meeting those requirements, and will define its current procedures for ensuring the confidentiality of the information it receives from the IRS in the Safeguard Security Report (SSR). Additionally, ITD will coordinate with Customers in filing Corrective Action Plans

(CAP) with the IRS, in order to communicate changes to enterprise architecture, policy, processes, and procedures as they develop in relation to systems that may utilize FTI.
7. ITD will maintain a list of employees authorized access. Such list will be provided to Customers and, upon request, to the IRS reviewing office.
8. No work specifically involving Federal Tax Information furnished under this agreement will be subcontracted without prior written approval of the customer
9. With respect to the supremacy of North Dakota Century Code (Chapter 54-59) describing the powers/duties and required use of ITD, customers will have the right to void this agreement if ITD fails to provide the safeguards described above.

## Criminal / Civil Sanctions

1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information 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 such returns or return information for a purpose or to an extent unauthorized 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. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of serving Customers. Information contained in such material 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 serving Customers. Inspection by or disclosure to anyone without an official need to know 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. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information 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 act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431.

3. Additionally, it is incumbent upon the contractor 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 contractors by 5 U.S.C.

552a(m)(1), provides that any officer or employee of a contractor, 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 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.

4. Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 4, *Sanctions for Unauthorized Disclosure,* and Exhibit 5, *Civil Damages for Unauthorized Disclosure*). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For both the initial certification and the annual certification, the contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

## Inspection

The IRS and Customers shall have the right to send its officers and employees into the offices and plants of ITD for inspection of the facilities and operations provided for the performance of ITD's services. On the basis of such inspection, specific measures may be required in cases where ITD is found to be noncompliance with required safeguards.