This agreement is based upon a mutual understanding between ITD and the IT Coordinators Council (reviewed June 24, 2016). In conjunction with ITD's Enterprise Service Level Agreement, it acts as a Service Level Agreement between ITD and all customers utilizing the Hosting service.

Contents

Infrastructure and Operations

ITD offers an environment for hosting enterprise services and line-of-business systems. It provides operational and infrastructure support that includes, but is not limited to, the following components:

Facilities

- A professional, raised floor datacenter equipped with redundant cooling and conditioned power which is supported by a UPS and diesel generator.
- Physical security is provided via a key card system with all access logged and monitored.
- Facilities comply with the Enterprise Architecture Physical Access Security Standard.

Hardware

- Solutions provided include rack space and professional-class server equipment designed for maximum availability with redundant components.
- Hardware is acquired with vendor supplied warranty and support.
- Hardware typically follows a 4-year replacement cycle.
- When appropriate, shared or virtual hardware is used in order to minimize costs.
- Hardware will be installed and configured in compliance with industry best-practices.
- Firmware updates will be installed as needed.

Operating Systems

- Distributed solutions are supported on multiple platforms in accordance with the Enterprise Architecture Server Operating Systems Standard.
- Anti-virus protection is provided in compliance with the Enterprise Architecture Anti-Virus/Spyware and Desktop Firewall Standard.

Storage

- ITD provides sufficient storage for operating systems, application software, and log files. Customers are generally billed by volume for application data.

Monitoring & Alerting

- ITD provides proactive monitoring of databases and hosted applications to ensure they are available for login. Customers must notify ITD if more extensive "beyond the application login" monitoring is required.
- Alerts are automatically reported as incidents to ITD's Service Desk on a 24x7 basis. Each incident is assigned a priority that drives ITD's resource commitment.

Load Testing & Performance Tuning

- All line-of-business web applications (written by ITD or purchased from a vendor) that run on shared ITD infrastructure must be load tested prior to production use in order to avert the risk of degrading server performance. ITD uses a variety of factors to ultimately determine if an application is performing at an acceptable level.

Load tests are performed prior to initially loading an application into production and prior to reloading a modified application into production. Cosmetic changes are exempt from the load testing requirement. ITD may also request load testing when upgrading infrastructure

components, such as hardware or operating systems. Rates for load testing are variable and will be based on the number of estimated users for the application.

- ITD monitors the performance metrics of the application environment and tunes the infrastructure for maximum performance and availability.

Availability

Ideally, availability should be measured end-to-end for an application within scheduled hours of operation. This approach is preferred over measuring individual components, such as database, network, and server availability, which would each have to be considerably higher to meet end-to-end levels.

ITD has the capability of providing end-to-end application monitoring for customers that are willing to incur scripting and licensing expenses. For all other services, uptime is determined by measuring the availability of a cluster of critical components and/or logon pages.

The following assessment shows industry levels of high availability and hours of unplanned downtime. It is based upon a white-paper published by Gartner, Inc. on September 26, 2014 (G00268541). The figures exclude planned downtime, which is agreed to by the customer in advance. Service disruptions caused by circumstances out of ITD's control (including deficiencies in vendor/customer software or acts of nature) may also be reported as a separate category.

Category	Availability Metrics	Unplanned Downtime Annually
Acceptable	99.50%	43.8 hours
Outstanding	99.80%	17.5 hours
Best in Class	99.98%	1.8 hours

ITD often provides what Gartner defines as Acceptable, Outstanding and even Best in Class service. However, specific IT architecture and infrastructure is required to ensure consistent availability at these levels. Customers must inform ITD of any application that requires critical or highly-critical levels of availability; by default, most applications are not architected in this fashion. Budgetary constraints typically constrain critical and highly-critical designations to systems that support public safety, health, finance, and/or legal obligations. Rates will be determined on a case-by-case basis.

Short and frequent outages could potentially cause availability metrics to appear adequate even as customer satisfaction declines. Therefore, the number of unexpected outages for a particular service must also be considered.

- Through best-effort support and component redundancy, ITD hosted systems typically achieve at least 99.50% (Acceptable) to 99.8% (Outstanding) availability and experience one or less unexpected outages per month.

- Through a highly-available architecture, requested and funded by customers, ITD hosted systems can predictably achieve at least 99.8% (Outstanding) to 99.98% (Best in Class) availability with four or less unplanned outages per year.

Data Backup

ITD provides data backup in accordance with the Enterprise Architecture Electronic Data Backup Standard. Data backups can cause significant load on system resource and measurably impact normal business operations. Therefore, the time for backups should be planned and agreed upon. Generally speaking:

- Daily off-site backups are provided for all data hosted and source-code written by ITD. Databases have full weekly backups and nightly incremental backups, while other datasets only backup items that have changed during the day.
- Standard backup configuration allows for a maximum of five different versions of each file to be stored within a 17 day window. A single version of the file will be retained even if it was done outside the 17 day window. Upon deletion from a system, the most recent version of a file is retained for 47 days before being completely purged from backup. The exception to this would be for Test Database backups as these backups are only kept for 15 days, not 47 days. Large-scale storage of static data typically warrants an alternative custom backup configuration.
- Data backups are optimized for Disaster Recovery purposes and are not intended to be used for records retention.

Service level objectives for backup reliability include:

- There will be less than two failed/canceled full or incremental backups per month
- Successful backups are expected 99.00% of the time, with a minimum of 95.00%
- Successful recoveries are expected 99.00% of the time, with a minimum of 95.00%

System Recovery

All hosted systems are designed with disaster recovery requirements as determined by the customer's business needs. Due to cost, most hosted applications are not architected by default for high-availability and/or business continuity. Therefore, it is the customer's responsibility to notify ITD of any specific Recovery Time Objectives (RTO) and/or Recovery Point Objectives (RPO) that exist.

A very limited subset of ITD hosted services have been architected for business continuity within their base rate. Specifically, RTO for enterprise systems include:

- 1 hour or less: Email, file and print services, and the AS/400 (iSeries)
- 4 hours or less: Drupal websites; does not inherently include linked applications
- 12 hours or less: Mainframe (zSeries) and ConnectND environments

In the event of a disaster, ITD will put forth its best-effort to restore service in a timely manner and to keep customers informed of progress. Customers retain responsibility for restoring associated end-user devices.

System dependencies and shared infrastructure may limit an individual agencies ability to conduct disaster recovery tests, declare a disaster, narrow RTO/RPO, and schedule roll-back after a disaster. Although custom disaster recover configurations are available upon request, agencies typically rely on data backup, data replication, or data replication with redundant processing:

Data Backup Only (Default)

Agencies that do not invest in replicated data solutions and redundant processing capacity will need to wait for additional storage and servers to be procured, for systems to be provisioned, and for data to be restored from backup. Restoration is dependent upon hardware availability, staffing priorities, system complexity/criticality, and the overall volume of data being restored from backup.

- RTO: 3-8 weeks
- RPO: 24 hour; data captured up to one day prior to the original outage may be lost

Data Replication

Replicated data improves disaster recovery by eliminating the dependency on restoration from backup. However, agencies that only invest in data replication would still need to wait for servers to be procured and for systems to be provisioned. Restoration is dependent upon hardware availability, staffing priorities, and system complexity/criticality.

- RTO: 2-4 weeks
- RPO: At or near real-time; minimal data loss prior to the original outage

Data Replication with Redundant Processing

Agencies that invest in both data replication and redundant processing capacity significantly improve their disaster recovery posture. Proactively orchestrating tasks and minimizing manual intervention also reduces staffing dependencies and system complexities during the recovery process.

Rather than investing in dedicated hardware, some agencies place test and/or development environments within the secondary datacenter with plans to re-provision them for production use in the event of a disaster. This approach carries the risk of being without non-production environments for an extended period of time; which may compromise an agency's ability to safely patch, upgrade, and test systems.

- RTO:

    - 48 hours or less if all dependencies require less than 48 hours to recover and if any dependencies require more than 12 hours to recover
    - 12 hours or less if all dependencies require less than 12 hours to recover and if any dependencies require more than 4 hours to recover
    - 4 hours or less if all dependencies require less than 4 hours to recover and if any dependencies require more than 1 hour to recover
    - 1 hour or less if all dependencies require less than 1 hour to recover
- RPO: At or near real-time; minimal data loss prior to the original outage

Database and System Administration

ITD supports databases on multiple platforms in accordance with the Enterprise Architecture Database Standard, the Enterprise Architecture Enterprise Database Security Standard, and the Enterprise Architecture Database Security Best Practices.

ITD is responsible for creating all User-IDs and database schemas in development, test, and production environments. ITD is also responsible for any structure changes in production and test environments, including:

- Creation of table-spaces, redo logs, and control files.
- Configuration of database parameters.
- Application of upgrade scripts.

Customers and their vendor(s) are encouraged to work closely with ITD's database administrators and security analysts when deploying and securing databases. In development and test environments, customers that are not utilizing ITD's Software Development staff are responsible for:

- Data modeling designs.
- Creation of schema database objects, including tables, views, indexes, procedures, triggers, functions, etc.
- Database tuning and performance testing before deployment to test and/or production.
- Setting up application and database security, and testing before deploying to production. This includes creating database roles and granting object privileges to roles.
- Monitoring batch processing jobs.

Customers shall contact ITD's Service Desk if the installation of an operating system or security patch is known to have an adverse impact on their application(s). The customer shall assume all risk associated with not installing the patch.

Production, test, and development environments do not inherently exist for all systems. When applicable, ITD is responsible for staging applications from Test to Production.

	Production			Test			Development		
	Primary Hours1	Extended Hours2	After Hours3	Primary Hours1	Extended Hours2	After Hours3	Primary Hours1	Extended Hours2	After Hours3
Response to high-priority automated alerts4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Recovery and restoration of backups	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Instance restarts to restore availability	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Instance restarts to implement planned changes5	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Patches and upgrades	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Planned changes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Emergency changes6	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No
Meeting attendance	Yes	No	No	Yes	No	No	Yes	No	No
Consulting and advise7	Yes	No	No	Yes	No	No	Yes	No	No

1Primary Hours: Monday – Friday, 8:00 AM to 5:00 PM

2Extended Hours: Monday – Friday, 7:00 AM to 8:00 AM and 5:00 PM to 10:00 PM

3After Hours: Saturday, Sunday, Holidays, and Monday – Friday from 10:00 PM to 7:00 AM

4Charges may apply to after-hour support if caused by user action or departmental coding errors.

5Database restarts during primary and extended business hours are included in the standard rate. However, charges may apply if business requirements mandate after-hour database restarts.

6Emergency changes during extended and after hours will be reviewed on a case-by-case basis to determine billing action.

7Extensive engagements may be charged a standard hourly rate.

Modifications

Date	SLA Modification
2016-06-24	Expanded System Restoration tiers and enhanced Availability benchmarks
2016-05-23	Converted from PDF to HTML format
2015-10-19	Redirected hyperlinks/endnotes to content on ITD’s new website
2015-04-13	Add RTO for Drupal Content Management System
2014-12-18	Redirected hyperlinks/endnotes to correspond with URL restructuring of EA standards
2013-02-05	Moved general Business Continuity into the Enterprise Service Level Agreement
2012-08-08	Significantly revised the Business Continuity section to more clearly articulate the current state
2011-01-07	Redirected hyperlinks/endnotes to content on ITD’s new website
2010-06-25	Updated ITD logo and added “State of North Dakota” / “Information Technology Department” to header
2010-06-22	Changed document title from “Hosting” to “Hosting Service Levels”