Office of Information Technology Services

Service Level Agreement

Distributed Hosting and Distributed Database Hosting

November 12, 2013

Distributed Hosting and Distributed Database Hosting

Service Description

Distributed Hosting

ITS Distributed Hosting provides dedicated and virtual hosting solutions for customer applications. Through the use of advanced technology, ITS provides multiple platforms geared to meet customer computing needs on a 24 x 7 basis. These platforms provide customers with highly available, monitored, and securely managed hosting solutions. The service design includes multiple redundant high-speed Internet connections, security protection, cooling/environmental system support and redundant power across two geographically-dispersed data centers. Supported hosting environments include:

- Windows and Linux hosting
- Virtual hosting services for Windows and Linux
- UNIX platform (Solaris, AIX)
- Virtual UNIX hosting support (Solaris, AIX)

Customers seeking hosting services are provided with provisioning/planning support, deployment coordination, OS patching and security, and monitoring of all hosted instances. ITS provides a single point-of-contact during planning/deployment as well as 24x7 operational support.

Distributed Database Hosting (Not included in the standard service offering)

Distributed Database Hosting provides the database infrastructure required to support business applications for your organization. In conjunction with the Distributed Hosting service, the DB team installs and maintains the database resource to ensure data integrity and security, as well as appropriate levels of availability and recoverability.

Distributed Database Hosting offers Standard and Extended Level Services. Extended Level Services include all Standard Level Services and are individually selected for specific needs of the client and their system's requirements. Support for each of the services offered in this area are quoted and charged separately. Additional details are provide in the Database Hosting Section of the ITS Service Catalog.

Storage and Backups

ITS offers a wide variety of storage capabilities to support Distributed Hosting, including tape, optical and disk. These capabilities span the mainframe and the distributed hosting environments, including both dedicated physical and virtual hosting offerings. ITS provides multiple disk and tape tiers such as high-end disk storage, virtual tape, mid-range disk storage, Network Addressable

Storage (NAS) devices, Serial Advanced Technology Attachment (SATA) disk systems, Storage Area Network (SAN) attached storage, and content addressable storage.

All hosting environments can be integrated with storage, backup, and archive services. Business continuity requirements for business critical applications and disaster recovery capabilities can be achieved via leverage of the geographically-dispersed Eastern and Western Data Centers, redundant high-speed networking, and enterprise backups and data mirroring across storage environments.

Backup/Data Recovery is available based on requirements. Standard media rotation and retention schedule is as follows:

- Daily incremental backups — retained off-site for two weeks
  - Daily incrementals are not retained longer than two weeks unless requested
  - Backups run Monday through Saturday
- Full backups are performed weekly and retained off-site for 1 month (1 copy per week)
- Backups moved off-site daily

Distributed Database Hosting Standard Level Services provides:
- Physical DB architectural design

- Installation and configuration of the DB engine

- Design and implementation of appropriate DB archive logs and backup schedule to provide for recovery objectives

- Maintenance level and security patches to the DB engine

- Scheduling services for recurring user-defined command scripts

- On-call paging and/or e-mail alert of DB resource availability and disk space

- Database recovery/restoration

Distributed Database Hosting Extended Level Services available:
- Database replication

- Database clustering

- Extended Production Problem Response up to 24 x 7

- Database migration assistance

Service Commitments

The general areas of support (such as Incident and Change Management) applicable to every ITS service, are specified in the ITS Global Service Levels document.

The Distributed Hosting target service availability is 99.99%.

Distributed Database Hosting's primary goal is to maintain the integrity and recoverability of the customer's data. ITS is committed to provide availability of the database service at 99% availability except during agreed upon maintenance windows as negotiated with the customer. Availability reporting and tracking will be accomplished by the completion of service requests in the Incident Management system indicating actual outage times. Database Hosting will work with the vendors to resolve all production database down issues with a 24x 7 effort.

Service Requests

Request Type	Example	Target Resolution Time
User Level	Change User Access Rights	Follows Incident Priority Model listed in the Global SLA
Server Level	Add memory or CPU	Follows ITS change process; Minor change is 3 days, significant change is 10 days and a major change is 30 days.
System/Application Level	Request to provision multiple servers and services in support of a new application.	Negotiated as part of the ITS Hosting Services Transition provisioning process.

Businesses Continuity and Disaster Recovery

ITS works with agencies and application owners to determine their recovery time objective (RTO), their recovery point objective (RPO) of their application and associated data and their method of recovery. This could include restores from application backups to new hardware, bringing the customers' development or pre-production environment up as production, or restoring the application on an existing platform that the customer has purchased as a cold or hot standby.

Database Hosting will provide resources to assist the customers during the annual Disaster Recovery test periods to recover their databases. The customer is responsible for procurement of the recovery hardware environment. The customer is expected to provide verification testing for all databases they request to be recovered during the exercise. Support for Disaster Recovery testing efforts outside the normal ITS spring and fall exercises are negotiated and scheduled in advance and are subject to time and material charges for effort exceeding 8 hours annually.

Data Backup and Retention Responsibilities

Database Backup, Retention, and Recovery requirements are defined by the customer during the provisioning process. Database Hosting services will configure database logging and backups to meet the customer recovery needs. Database backups are scheduled, performed and monitored by the Database Hosting services group. Service level is set at 100% of daily backups executed without error. Reporting of backup daily backup execution status is available to the client by database mail as a component of the backup batch process.

Hours of Availability

The Distributed Hosting service is available 24 x 7 and adheres to the maintenance window schedule listed in the ITS Global Services Section document. Support is available 7 days a week, 24 hours a day and 365 days a year by contacting the ITS Service Desk.

Distributed Database Hosting standard support hours are from 8:00 a.m. to 5:00 p.m., Monday-Friday. Extended support up to 24 x 7 with on-call paging is available as required for production instances.

ITS Responsibilities

Support and Maintenance

Support and maintenance includes hardware, operating system, performance and system monitoring, and security vulnerability and scanning.

Hardware support and maintenance

- ITS installs and sets up all server hardware in accordance with industry best practices. Also, in conjunction with the hardware operating system (OS) vendors, ITS will apply firmware patches to systems in accordance with state policies and standards.

- ITS also repairs or replaces any hardware component under warranty shown to be defective; predictive analysis indicates an impending failure or not performing as designed.

- ITS follows the Prioritization Model specified in the ITS Global Service Levels for incident and request status reporting intervals and target resolution times.

Operating system support and maintenance

- ITS, at the recommendation of the ITS Enterprise Security and Risk Management Office (ESRMO) and OS vendors, will apply patches to operating systems in accordance with state policies and standards.

Distributed Database Hosting

- Distributed Database Hosting will provide resources to assist the customers during the annual Disaster Recovery test periods to recover their databases. The customer is responsible for procurement of the recovery hardware environment. The customer is expected to provide verification testing for all databases they request to be recovered during the exercise. Database Hosting recovery objectives follow the standard ITS RTO objectives. Support for Disaster Recovery testing efforts outside the normal ITS spring and fall exercises are negotiated and scheduled in advance and are subject to time and material charges for effort exceeding 8 hours annually.

- Database Backup, Retention, and Recovery requirements are defined by the customer during the provisioning process. Database Hosting services will configure database logging and backups to meet the customer recovery needs. Database backups are scheduled, performed and monitored by the Database Hosting services group. Service level is set at 100% of daily backups executed without error. Reporting of backup daily backup execution status is available to the client by database mail as a component of the backup batch process.

Performance and system monitoring

- ITS monitors key items for all servers on the following platforms:
  - Linux — See Linux monitoring parameters and notifications.
  - UNIX — See UNIX monitoring parameters and notifications.
  - Windows — See Windows monitoring parameters and notifications.
- ITS monitors processes and log files, as requested

- ITS performs standard fault, configuration, performance and security management monitoring of the Server Farm Network including:

- o Fault detection with notification to operational personnel, customer contacts and incident ticket creation
- o Intrusion prevention monitoring and automated ticket generation
- o Archiving device configurations and insuring security policies are enforced in the configuration
- o Syslog collection and archiving
- o Network device authentication, authorization and accounting

Security, vulnerability and scanning

- ITS perform periodic scans of IP addresses under the State of North Carolina's control:
  - o ITS takes every precaution to protect the network infrastructure and the machines scanned.
  - o Scans are run in the safe mode ensuring minimum impact.
  - o Enterprise Security and Risk Management Office (ESRMO) coordinates and communicates scans following the ITS Change Management process.
  - o ESRMO provides a notification email prior to performing a scan.
  - o If an agency does not want an application scanned, the customer will need to follow the Statewide Standards Deviation Reporting process (040106).
  - o ITS makes no representation or warranty that vulnerability scans will disclose all vulnerabilities.
- ITS provides consultation on findings and mitigations
- ITS tracks findings according to classification and status

Systems Administration

ITS will make every effort to provide agency administrators the ability to perform system level functions in support of their application, Access to the required commands will be limited through the use of the pseudo command or permissions granted through the use of group policies. To retain control and accountability, ITS will not grant root or administrative access to administrators or users outside the ITS Distributed Hosting group.

Customer Responsibilities

Agency Application Lifecycle Management

- Application information gathering and documentation is the responsibility of the business system owner. The business system owner is responsible for engaging the agency security liaison, agency technicians, vendors, and others as required. ITS is available to facilitate the gathering of requirements and templates.

- The agency is responsible for the life cycle of the application which includes application patching and working with ITS staff to patch the operation system.

Database Responsibilities

- Customers are responsible for providing and maintaining their own application and application DBA support. Database ownership rights are assigned to the customer; Database Hosting services retains systems configuration and administration rights.

- Customers should notify the DBA services group, through the ITS Service Desk, of any planned application and/or database changes that will affect the database structure before changes are made

- Customers should designate local staff to serve as the primary contact for the database hosting services group

- Customer support requests should be directed to the ITS Service Desk

- Customers are expected to perform verification tests after all database patching and maintenance activities

- Database Backup, Retention, and Recovery requirements are defined by the customer during the provisioning process

- The customer is responsible for all database archive and purging activities

- The customer is responsible for procurement of the recovery hardware environment

Communications with ITS

- Contact the ITS Service Desk:
    - When changes are being applied to your applications
    - When application changes are slated to be applied that may conflict with the ITS standard maintenance window
    - When the installation of a mandatory OS or security patch is known to have an adverse impact on a customer application(s). ITS will work with the customer and make every effort to eliminate or mitigate the impact of the patch. If the customer chooses not to install the patch, a deviation request must be submitted by the customer to the Enterprise Security and Risk Management Office.

- Provide a list of approved customer contacts who can request changes to the application environment to the ITS Service Desk. This list should include contacts for both standard business hours and 24 X 7 support.

Risk Management

- Conduct Risk Management:

- o Agencies should identify the potential risks and impacts to service delivery from either application or hardware failure to develop the strategies, justify the resources required to provide the appropriate level of Business Continuity services and develop a test plan to verify the strategy is sufficient to recover the business in the event of a failure.

- o Agencies should conduct business risk analysis activities that clearly define the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for all business critical systems. Suggestions to include:

  - Define the agency's critical functions and services

  - Define the resources (technology, staff, and facilities) that support each critical function or service

  - Identify key relationships and interdependencies among the agency's critical resources, functions, and services

  - Estimate the Recovery Point Objective (RPO) - the maximum amount of information or data that can be lost without a catastrophic impact to critical function or service.

  - Estimate the Recovery Time Objective (RTO) -. maximum amount of hosting services downtime without a catastrophic impact to critical function or service.

  - Identify any interim or workaround procedures that exist for the agency's critical functions or services

- Work with ITS to define a backup strategy and determine retention requirements.

- Remediate security findings in accordance with Statewide Information Security Standards or accept the risk and follow the approved Statewide Standards Deviation Reporting process.

Service Level Agreement Scope

This agreement specifies only the standard operational service commitments and responsibilities of ITS and its customers. Customer-specific deviations from these commitments and responsibilities will be specified in an accompanying Memorandum of Understanding. Service rates are outside the scope of this agreement and are specified in financial documents.

Signatures of Approval and Agreement Date

Customer Signatures

Agency Head or Designee:

Name	Title	Signature	Date

Agency Chief Financial Officer:

Name	Title	Signature	Date

ITS Signature

State Chief Information Officer:

Name	Title	Signature	Date
Chris Estes	State CIO		