State of North Carolina
Department of Information Technology

Service Level Agreement
for

Enterprise Directory Services

November 6, 2017 v2.2

Enterprise Directory Services

Service Description

Enterprise Active Directory provides a centralized authoritative repository of information about network-based resources (such as computers, printers, applications, and file shares). It simplifies the management of these resources while controlling who can access them.

Agencies integrated into the Enterprise Directory Service can take advantage of single/simplified sign-on by accessing all network-based resources using their NCID username and password.

Agencies can also take advantage of the Enterprise Shared LDAP environment. This environment allows applications anywhere in the state to securely authenticate any user who has an NCID account. This provides a simple methodology for applications to securely authenticate users without additional infrastructure costs or complexity.

The Enterprise Directory Service Team assists customers in migrating to the Enterprise Directory by utilizing a proven repeatable process, highly rated migrations tools and years of experience. This saves the customer both time and money as they move from older platforms into the Enterprise Directory.

The core support of the Enterprise Directory is managed by the Enterprise Directory team. Customers maintain and control the support of applications, data, printers, servers and computers.

Active Directory Communication

Network communication between the customer's subnets and the Enterprise Directory subnets must be modified to allow Directory and associated client and service communication.

Information reviews will be established between Directory Services and the Agency to make sure that both groups are aware of technology directions, business changes and upcoming projects that would have an impact on the environment.

To engage the Directory services group in Directory-related issue or needed change, please call the DIT Service Desk and open a service request for the Enterprise Directory Services Team.

Service Commitments

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

- Enterprise Active Directory Service Availability Target – 99.99%
- RTO (Recovery Time Objective) - EAD will be back online within 30 minutes should a full data center outage occur at one of the state's two data centers. EAD will be able to handle the full production load, but performance may be diminished somewhat until the other data center is restored.

Hours of Availability

This service is available to customers 24 x 7 and adheres to the maintenance window schedule listed in the DIT Global Services document.

Directory Service Responsibilities

In the Enterprise Directory environment and other directories, the team supports, they will be solely responsible for the maintenance and control of the Active Directory infrastructure, specifically:

- Overall Forest and Domain architecture, design and maintenance.
- Domain Controller Implementation, Security and Management; Schema Management; Group Policies; Replication Topology; Sites and Services; Trust Relationships; DNS; OU Design and Management; Delegation of Rights; Built-in Group Management; Forest and Domain Security; Directory-Based Account Management.
- The creation and subsequent applying of customer specific GPO's is done collaboratively between Directory Services and the customer. The customer will be responsible for either the creation of agency specific policies or working with the Active Directory team to assist in developing agency specific policies. The DIT Directory Services team is solely responsible for applying all customer GPO's to the Enterprise environment
- Active Directory System State backups and restores.
- Participation in scheduled Disaster Recovery and Business Continuity Plan testing as required.

Customer Responsibilities

Customer support staff will have the following delegated responsibilities:

- Administrative control and responsibility for application servers and associated data
- Administrative control and responsibility for file/print servers and associated data
- Administrative control and responsibility for client machines and devices
- Responsible for backup and restore of application and file/print server data
- Responsible for support and maintenance of all non-Windows products that are connected to the Enterprise Directory
- Responsible for the definition, testing and approval of agency-specific GPO's
- User management such as creation of new accounts, removal of existing accounts and password management is done through NCID and not directly performed in the directory. The customer is responsible for managing these activities through the NCID management portal.
- Customer support staff will have delegated administrative rights within the Enterprise Active Directory portal for group management as well as the ability to add/remove devices, such as workstations and servers
- The customer is responsible for working with Directory Services to anticipate changes in service demands prior to the purchase of any new application or hardware that may have an impact on the Enterprise.

Service Level Agreement Scope

This agreement specifies only the standard operational service commitments and responsibilities of DIT 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

DIT Signature

State Chief Information Officer:

Name	Title	Signature	Date
Eric Boyette	State CIO		