Identity Management - Active Directory
Service Level Agreement (SLA)
By
Information Technologies (UNM IT)
For
University of New Mexico (Customer)

Effective Date:	1/1/2016
Document Owner:	Brian Pietrewicz

Related/Referenced Documents:

Table of Contents

1   General Overview

This is an SLA between the Customer and UNM IT to document the provision of:

- The Active Directory;
- The general levels of response, availability, and maintenance associated with these services;
- The responsibilities of UNM IT as a provider of these services;
- The responsibilities of the End-Users and Customers receiving these services;
- The financial arrangements associated with the service.

This SLA shall be effective as of the Effective Date set forth on the cover page and will continue until revised or terminated.

2   Service Description

UNM IT documents services and associated fees in the UNM IT service catalog.

The Active Directory (AD) service provides a single, consistent point of access management for users, applications, and devices. All data is hierarchical, replicated and extensible. AD is used for managing permissions and user access to network resources. Simplified management and use of file and print services make network resources easier to find, configure and use. UNM NetID is synchronized between AD and other university directory services (LDAP) providing seamless authentication to enterprise services. Single sign-on experience for services integrated with UNM enterprise Active Directory and delegated full control to IT administrators for their department organization unit (OU) to create and manage computers, groups, group policies and sub OUs. Department IT resources will be provided an initial onboarding and ad hoc monthly OU Administrator training from UNM IT.

2.1   Service Scope

This SLA will define the technical requirements, boundaries and service levels between UNM IT and UNM Department IT staff to successfully utilize AD.

Active Directory features include:

- Full control of department's organizational unit (OU);
- Ability to create custom groups, computer objects, group policies, child objects, for departmental OU;
- Seamless authentication to university enterprise services connected to Active Directory. Example: SharePoint, File Shares, and O365 components;
- Lower departmental costs, freeing valuable IT resources to allow staff to focus on delivering department specific services;
- NetID synchronization between AD and other enterprise directory services (LDAP);
- Improved security including Kerberos authentication, automatic updates (Windows System Update Server), intrusion detection, and centralized monitoring;
- Monthly training for OU Admins;
- Banner roles converted into AD Groups.

2.1.1   End-User Requirements to Use the Service

- OU Administrator or Department IT is responsible for first level triage of incidents and service requests;
- OU Administrators will attend UNM IT provided AD training;

- OU Administrators will adhere to the standards, policies and guidelines included in the OU Admin training such as the naming convention and use of privileged accounts;
- OU Administrators will link and manage their OU group policies;
- Manage their OU with an OU Administrators group consisting of department IT staff or their delegate;
- Administrative control for all servers, associated data, client machines and devices.

2.1.2 Boundaries of Service Features and Functions

- OU Administrators are limited to only managing their own OU;
- UNM IT retains administrative access to forest and domain level operations;
- UNM IT reserves the right to apply security policy settings through domain GPO with reasonable notification;
- Services hosted by UNM IT are being provided to the Department IT only. Any resale of this service must be disclosed in advance, in writing to UNM IT;
- Any features not covered by this SLA may incur charges. Please refer to UNM IT Service Catalog for additional information;
- User management such as creation of new accounts, and password management is done through NetID service and not directly performed in AD.

2.2 Service Level Performance

2.2.1 General Service Levels

- Response to reported incidents and service requests as defined in Sections 5 and 6 below;
- OU Admin training customized to UNM IT infrastructure;
- Network security scans are completed for all systems slated for AD migration;
- Default policies configured for Department IT OU.

2.2.2 Specific Service Levels

- Backup of AD infrastructure, retained for 30 business days;
- Active Directory Service is natively load balanced to provide 99.9% uptime.

3 Roles and Responsibilities

3.1 UNM IT Responsibilities in Support of the Service

UNM IT responsibilities and/or requirements in support of this SLA include:

- 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 (Domain Name Service); OU design and management; delegation of rights; built-in group management; forest and domain security; directory based account management;
- The creation, notification and subsequent implementation of customer specific GPOs is completed by UNM IT upon request by Department IT;
- Active Directory system state backups and restores;
- Participation in scheduled Disaster Recovery and Business Continuity Plan testing as required;
- Document services provided in UNM IT service catalog;
- Notify the Department of any situation in which extra time is being required of UNM IT staff due to lack of Department staff knowledge, planning or poor implementation practices. UNM IT reserves the right to bill, at our standard hourly rate or expedited service rate, for this additional support;
- Communicate any changes to services to the appropriate UNM audience;
- Publish all scheduled maintenance via:

- o IT Alerts at http://it.unm.edu;
- o LoboMobile;
- o SYSINFO-L listserv email.

3.2 Customer Responsibilities in Support of the Service

Customer responsibilities and/or requirements in support of this SLA include:

- Notify UNM IT of special types of data that are being collected (i.e. secure/confidential, PII, FERPA, HIPAA), or whenever new special types of data are planned to be collected;
- Provide a representative to discuss high-priority incidents that may arise; and attend high-priority incident reviews;
- Mitigate any issues identified via security or virus scans, prior to migration;
- Utilize UNM IT Service Desk for incidents;
- Ensure staff is familiar with the provisions of this SLA;
- Maintain appropriate staff expertise in the maintenance and support of any Customer supported equipment and/or applications;
- Request access to UNM IT billing portal for appropriate staff;
- Review UNM IT Billing Portal on a monthly basis and submit any billing inquiries within 90 days;
- Comply with UNM Business Policies 2500, 2520, 7215.
  - https://policy.unm.edu/university-policies/2000/2500.html
  - https://policy.unm.edu/university-policies/2000/2520.html
  - https://policy.unm.edu/university-policies/7000/7215.html

4 Hours of Coverage and Escalation

4.1 Hours of Coverage

Active Directory is provided 24 hours a day 7 days a week except for periods of planned maintenance, UNM holidays, catastrophic events or Campus closures.   Support for Active Directory service requests will be handled Monday through Friday from 8am to 5pm.

4.2 Service Exceptions to Coverage

This section intentionally left blank.

4.3 Escalation and Exceptions

If you are not satisfied with the performance of the service or incident/request process, please contact the Service Owner or Service Manager.

UNM IT Contact	
Service Owner	Brian Pietrewicz Director, IT Platforms 505-277-0260 bpietrewicz@unm.edu
Service Manager	Ann Swancer Associate Director, Customer Support Services aswancer@unm.edu 505-277-0622

To request exceptions to defined service levels based on exceptional business needs, please email cio@unm.edu. The Office of the CIO/UNM IT will respond to the message within 5 business days and escalate any mutually agreed upon exceptions to the appropriate Department Executive Vice President and UNM's Senior Administration for review, approval, and funding, if necessary.

5 Service Requests

A Service Request is defined as a request for information, advice, or for access to a service.

5.1 Service Request Submission

Service Requests can be submitted by calling 505.277.5757. Current hours of operation are listed on the Customer Support Services website, http://it.unm.edu/support.

Online Service Requests can be submitted at the following URL: https://help.unm.edu.

5.2 Service Request Response

For all requests, UNM IT's objective is to acknowledge and assign requests within twelve (12) business hours of receipt. Requests will be fulfilled within seven (7) days.

Campus priorities may require exceptions during certain times of the Academic year.

6 Incidents

An incident is defined as any interruption in the normal functioning of a service or system.

6.1 Incident Report

Incidents can be reported using Help.UNM at https://help.unm.edu or by calling the UNM IT Service Desk during business hours at 505.277.5757.

For service outages after hours, call 505.277.5757 and select Option #3 to leave a message for the Manager on Duty (MOD). The MOD will contact the appropriate service technician to help resolve the service outage.

Time spent on resolving incidents that are end-user caused will be billed to the appropriate party at current hourly rate, including travel time. Material will be billed along with any associated expenses incurred to remedy the Incident.

6.2 Incident Response

Response time objectives for incidents reported to UNM IT are as follows:

Priority 1 (P1) is acknowledged, accepted and resolved within four (4) clock hours.

Priority 2 (P2) is acknowledged, accepted and resolved within one (1) business day.

Priority 3 (P3) is acknowledged, accepted and resolved within four (4) business days.

Priority 4 (P4) is acknowledged, accepted and resolved within nine (9) business days.

.

6.3 Prioritization

All reported incidents receive a priority number based on the impact and urgency of the service interruption.

Impact is determined based on the number of people/departments/buildings that are affected by the interruption or outage. Life-Safety issues are taken into consideration for assessing and assigning priorities.

Urgency is based on the acceptable delay to restore the service. Urgency can be critical or high and is determined based on the nature of the service outage.

UNM IT may prioritize incoming incident requests as P1 or P2 priority if it meets one or more of the following criteria:

- Significant number of people affected;
- The level to which work is impaired for individuals;
- Academic and Administrative Calendar deadlines;
- Significant impact on the delivery of instruction;
- Significant risk to safety, law, rule, or policy compliance.

7   Maintenance and Service Changes

The Maintenance Window for Active Directory can be found on the UNM IT website, http://it.unm.edu/availability.

UNM IT reserves the right to modify the maintenance window.

8   Pricing and Billing

Charges for UNM IT services are billed monthly in arrears and post automatically to UNM departmental indices on the 1st business day of each month. Monthly bill detail for UNM IT charges can be accessed using the UNM IT Billing Portal at http://it.unm.edu.

9   Reviewing and Reporting

9.1   System Performance and Availability Reporting

Service performance and availability reports can be provided upon request.

9.1.1   Downtime Criteria

The following criteria will be used to calculate downtime for Active Directory:

Any unscheduled period of time in which Active Directory is unable to authenticate or authorize accounts. Approved scheduled maintenance windows will not count towards downtime.

9.2   SLA Reviews

UNM IT is responsible for facilitating reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties.

This SLA contains the complete agreement between the parties and shall not be changed, amended or altered except in writing and signed by each party.

10 Approvals

UNM IT: University of New Mexico CIO   **CUSTOMER:**

By: Gilbert Gonzales_____   By:_____

Title: Chief Information Officer___   Title:_____

Signature:_____   Signature:_____

Date:_____   Date:_____