UNM **Information Technology**

UNM Active Directory Standard

IT Standard Issued: 2008
Supersedes: New Standard

Responsible Executive: Arthur Bernard Maccabe, UNM Chief Information Officer

Responsible Office: UNM Office of the Chief Information Officer

Contact: For questions about this standard contact ADTC-L@List.UNM.Edu

Summary of Standard:

This standard defines the requirements to install and support Windows Active Directory services at the University of New Mexico, hereafter referred to as the "UNM Enterprise AD Network".

- Specifies the Active Directory topology for the UNM Enterprise AD Network.
- Sets forth roles, responsibilities and requirements for the Active Directory Technical Committee, IT, and UNM colleges, departments and other UNM affiliated organizations implementing Active Directory services.
- Establishes a single forest design where all organizational entities subject to UNM's authority implementing Active Directory will reside.

Who is affected by this Standard?

This standard applies to any UNM organizational entity (i.e. college, school, department, business unit, or other UNM affiliated organization), hereinafter referred to as a "department", that intends to implement, or has implemented Active Directory within the UNM Enterprise AD Forest.

Why we have this Standard?

The Active Directory Standard enables the development of an effective, scalable, secure and manageable Active Directory forest design and facilitates one standardized infrastructure for the UNM forest**.** This will enable campus wide Windows services, consistent support of university security and identity management standards, and reduce total cost of ownership for UNM network operations.

Given the distributed nature of Active Directory and the potential for wide use of the campus Active Directory forest by the university IT community, the purpose of this standard is to assure continuity, reliability, and sustainability of both services and resources.

Responsibilities:

The **Active Directory Technical Committee** (ADTC) shall govern the design, implementation, and operation of Active Directory on UNM's Enterprise AD Network and as specified in the Specifications below. The ADTC is comprised of experienced campus Active Directory administrators, appointed by the CIO, with extensive knowledge of Active Directory and the services it provides. The ADTC is the governing body for designing, evaluating, and engineering forest wide changes to the UNM Enterprise AD Forest. ADTC will:

- Plan, design, and implement the UNM enterprise AD forest.
- Manage all technical and functional aspects for the Active Directory forest.

- Maintain this standard.

Develop, maintain, and review processes necessary for departments to participate in the UNM Enterprise AD Network and utilize Windows and Active Directory services. These procedures and processes are documented in the UNM Windows Server 2008 Active Directory Design document, UNM AD Migration Checklist for Departments, UNM AD Naming Convention and this standard.

The UNM Offices of the CIO charters IT with the ongoing responsibility for the operation, administration, and support of the UNM enterprise Active Directory forest on behalf of the ADTC including:

- Support of UNM enterprise Active Directory as a sustained UNM IT service.
- Provisioning and maintaining platform infrastructure and core enabling licensing (server and client) necessary for UNM-wide Active Directory deployment.
- Monitoring, troubleshooting, and resolving problems with enterprise Active Directory services. These responsibilities include but are not limited to fielding trouble notifications, providing proper documentation of these activities, defining escalation procedures and primary service points of contact in accordance with standards and procedures, analyzing and reporting performance data, and problem troubleshooting and resolution.

Participating **UNM Organizational Entities** (i.e. colleges, schools, departments, business unit, and other UNM affiliated organizations) will:

- Comply with all UNM Enterprise AD standards and procedures.
- Manage and operate departmental Active Directory domains and OUs in adherence to ADTC standards and procedures.
- Provision, operate, and maintain departmental domain controllers and other departmental Windows services infrastructure.
- Monitor, troubleshoot, and resolve problems with departmental Windows and Active Directory services.
- Acquire and maintain necessary server and client licensing for department level Windows and Active Directory services not provided by IT.

Specifications:

1. **UNM Enterprise AD Forest Structure**

   There is one enterprise AD forest structure for UNM. IT is responsible for the management and operation of the enterprise forest root domain on behalf of the ADTC.

   The UNM Enterprise AD Network design is structured to take advantage of the flexibility of domains and organizational units (OUs) in Active Directory. An empty forest root is implemented to maximize security and allow child domains to be reorganized. A single forest design is employed to reduce costs, ease administration, and provide the foundation for the deployment of integrated services.

   All OU designs are governed by the UNM Windows Server 2008 Active Directory Design document.

2. **Windows Services**

   IT will be responsible for maintaining enterprise Windows and Active Directory services to ensure business continuity for participating departments. Requests for Windows service related enterprise schema modifications and security policy changes must be approved by ADTC and will be implemented by IT.

3. **Domain Plan**

There will be a single, dedicated root domain for the UNM Enterprise AD forest. This will provide a controlled environment for forest wide change management and limit the amount of replicated data. The root domain will contain no user accounts and will be used strictly as an empty domain to manage the schema, global catalog, site topology, security and enterprise policy. Please refer to the UNM Windows Server 2008 Active Directory Design document for detailed domain plan.

4. **Domain Control and Security**

Membership in the enterprise forest root domain, schema, enterprise, and domain administration groups is restricted and controlled by ADTC. ADTC will maintain a high level of security on all levels to ensure only properly authorized changes are implemented. ADTC will maintain proper change control and audit mechanisms.

5. **Domain Name Service (DNS)**

The primary Active Directory DNS zone for UNM is owned and managed by IT on behalf of the ADTC. Active Directory DNS is managed in compliance with established UNM standards and procedures for DNS. DNS support for UNM Active Directory appears as a stub zone in primary DNS and is replicated between all Active Directory DNS servers in the enterprise forest root domain. Departments may create and manage sub zones to the Active Directory zone in accordance with ADTC prescribed standards. All Active Directory DNS zones will be implemented as Active Directory integrated zones where possible.

6. **Organizational Unit (OU) Plan**

Each department manages its objects in their department OU, while the ADTC manages the configuration of the directory service.

7. **Organizational Control**

Participating departments are responsible for the management and operation of their own organizational units in compliance with ADTC standards and responding to requests for creation of all organizational units within its sub-domain. Alternatively, departments may choose to enter into an agreement with an ADTC approved UNM IT provider to perform these services on behalf of the department.

8. **Organizational Management and Site Control**

Departments will designate an OU manager for organizational unit. Each OU manager must be a regular/non-temporary UNM employee. The OU manager controls a sub-tree of objects in Active Directory. Departments will develop and adhere to department site control procedures in compliance with ADTC standards. Departments may alternatively enter into agreements with an ADTC approved UNM IT provider to manage and operate departmental OU services.

9. **AD Sites and Services Plan**

Designing network topology is the responsibility of the respective UNM Network Group. The ADTC will consult with and advise UNM Network Groups regarding network topology and AD design. IT on behalf of ADTC is responsible for configuring AD Sites and Services based on the network topology and placing AD services accordingly.

10. **Backup and Disaster Recovery**

Backup and recovery of the forest root domain will be the responsibility of IT on behalf of ADTC In accordance with approved ADTC backup and recovery procedures.

11. **Directory Replication**

    Replication of the enterprise forest root domain will be the responsibility of IT on behalf of ADTC.

12. **Availability**

    IT will provide at least three domain controllers for the root forest directory.

Mandatory Procedures: [Include minimum required standards.]

Defined in the Premigration Checklist and UNM AD Naming Convention documents.

Recommended Procedures: [Include any additional recommended standards.]

See above.

Exceptions:

The ADTC evaluates and makes recommendations on requests for exceptions to this standard. The Office of the CIO is the only entity that can grant exceptions to this standard and will do so only after consultation with and recommendation of the ADTC. There is a single explicit exception made for private test, research and development networks that are physically and electronically discontinuous from all other UNM and off-campus networks.

Website Address for this Standard: http://cio.unm.edu/standards/

Related Documents: Policy 2560 “IT Governance,” Policy 2500 “Acceptable Computer Use,” Policy 2510 “Computer Use Guidelines,” Policy 2520 “Computer Security Controls and Guidelines,” and/or Policy 2590 “Access to Administrative Computer Systems.”

Glossary:

Domain: In Windows 2003 and Active Directory, a collection of computers defined by the administrator of a Windows 2003 server network that share a common directory database. It provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has its own security policies and security relationships with other domains.

Schema: The definition of an entire Active Directory database; the universe of objects that can be stored in the directory is defined in the schema. For each object class, the schema defines what attributes an instance of the class must have, and what object class can be a parent of the current object base.

Domain Name Service: Domain Name Service (DNS) is a hierarchical distributed database used for name/address translation and client server rendezvous. Domain Name Service is the namespace used on the Internet to translate computer and service names into TCP/IP addresses. Active Directory uses DNS as its location service that enables clients to find domain controllers using DNS queries.

Sub-Domains - Any child of a domain zone.

AD Site: An AD site is defined as one or more well connected TCP/IP subnets that participate in the UNM Enterprise AD network.

Appendices:

UNM AD Naming Convention
UNM AD Migration Checklist for Departments
UNM Windows Server 2008 Active Directory Design