USC Active Directory Operations Guide

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Date (MM/DD/YYYY)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iv</td>
<td></td>
<td>11-25-07</td>
<td>Working Draft after 11/15 Working Group Review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2-25-08</td>
<td>Updated OU Admin Form</td>
</tr>
</tbody>
</table>

Table of Contents

1 Introduction .................................................................................................................. 4
2 Glossary of Terms ....................................................................................................... 5
3 Roles ............................................................................................................................ 6
4 Organizational Unit Structure .................................................................................... 8
5 Managing the Active Directory Hierarchy ..................................................................... 10
   5.1 Responsibilities of AD Administrators ................................................................. 10
   5.2 Enforcing Compliance ............................................................................................ 11
       5.2.1 Categories of Offenses .................................................................................... 11
       5.2.2 Consequences and Escalation .......................................................................... 11
       5.2.3 Exceptions ....................................................................................................... 12
   5.3 Enterprise and Domain Administration ................................................................. 12
   5.4 Organizational Unit Administration ....................................................................... 13
       5.4.1 Delegation of an Area OU .............................................................................. 13
   5.5 Delegation of Sub-OU’s ........................................................................................ 13
   5.6 Best Practices for Structuring an OU .................................................................... 14
6 Naming Conventions ...................................................................................................... 15
   6.1 Standard Prefix ..................................................................................................... 15
   6.2 Registering a Standard Prefix ................................................................................ 15
   6.3 Device Names ....................................................................................................... 16
   6.4 Group Names ....................................................................................................... 16
   6.5 Group Policy Names .............................................................................................. 16
   6.6 E-Mail Distribution Lists ....................................................................................... 16
   6.7 Requesting an E-Mail Distribution List .................................................................. 17
   6.8 User Account Names ............................................................................................. 17
   6.9 Resource Account Names ...................................................................................... 17
7 User Accounts and Provisioning .................................................................................... 18
   7.1 Student Accounts .................................................................................................. 18
   7.2 Employee Accounts .............................................................................................. 19
       7.2.1 Expediting an Employee Account ................................................................. 19
       7.2.2 Adjunct Employee Accounts ......................................................................... 19
   7.3 Retiree Accounts ................................................................................................. 20
       7.3.1 Requesting or Renewing a Retiree Account ..................................................... 20
   7.4 Affiliate Accounts ............................................................................................... 20
   7.5 Admin Accounts .................................................................................................. 20
   7.6 Resource Accounts ............................................................................................. 21
7.7 Guest Accounts.................................................................21
7.8 Account Management ......................................................22
  7.8.1 Requesting a Larger Mailbox for an Employee ......................22
  7.8.2 Requesting a Username Change ......................................22
  7.8.3 Terminating or Administratively Disabling Accounts ...............22
  7.8.4 Retaining E-Mail for Employees Who Have Terminated ............23
  7.8.5 Continuing Accounts for Employees Who Have Terminated ........23
8 Groups Provisioning ..............................................................23
9 Management of Groups .........................................................25
  9.1 Types of Groups ..............................................................25
  9.2 Group Scope .................................................................25
  9.3 Creating and Managing Groups ..........................................26
  9.4 Mail Enabling Groups ......................................................26
10 Group Policy ........................................................................27
  10.1 Overview .........................................................................27
  10.2 Who can create group policy .............................................27
  10.3 Examples of Group Policy ................................................27
  10.4 Group Policy Status Setting ..............................................28
  10.5 Using Group Policy Loopback Processing ................................28
  10.6 Maintenance of group policy ..............................................29
    10.6.1 OU Administrators’ Responsibility .................................29
    10.6.2 Oversight Committee Audit .........................................30
    10.6.2.1 Shared Policies ......................................................30
    10.6.2.2 Non-Shared Policies ..............................................30
  10.7 Establishing a Shared Policy ..............................................31
  10.8 Current Domain Policy in Effect ........................................31
11 Migrating to AD and Exchange ..............................................32
  11.1 Manual Desktop Migration ...............................................32
  11.2 Joining Macintosh Computers to AD ....................................33
  11.3 Server Migration ............................................................33
  11.4 Departmental Application Migration ....................................34
  11.5 E-Mail Migration ............................................................34
    11.5.1 Migration from GroupWise .........................................34
    11.5.1 Migration from Exchange ...........................................35
    11.5.1 Migration from Other E-Mail Systems ............................36
12 Data Access .........................................................................37
  12.1 HR Data ..........................................................................37
  12.2 Student Data .....................................................................37
13 Administrative Tasks and Oversight ........................................38
  13.1 OU Administration Tasks – Operational (No Reporting, No Oversight Approval) ...38
  13.2 OU Administration Tasks – Reporting Requested (No Approval Required) ..........38
  13.3 OU Administration Tasks – Oversight Approval Required ................38
  13.4 Enterprise Administration Tasks – Operational (No Reporting, No Oversight Approval) .........................................................39
  13.5 Enterprise Administration Tasks – Reporting Required ................39
  13.6 Enterprise Administration Tasks – AD/Exchange Oversight Approval Required ...39
14 USC Active Directory & Exchange Oversight Committee ................40
  14.1 Scope of Responsibility ...................................................40
  14.2 Authority ........................................................................40
  14.3 Membership ....................................................................40
  14.4 Decision Process ............................................................41
  14.5 Meeting Schedule ...........................................................41
  14.6 Request Submission & Approval Process ..............................41
14.7 Incident / Problem Management Process ......................................................... 42
14.8 Appeals ........................................................................................................ 42
14.9 Committee Audit .......................................................................................... 43
15 User Support .................................................................................................... 44
15.1 Available Information .................................................................................... 44
15.2 Password Resets ........................................................................................... 44
15.3 Shared Support Model .................................................................................. 44
16 System Configuration Defaults ......................................................................... 46
17 References ......................................................................................................... 47
Appendix A ............................................................................................................ 48
1 Introduction

USC initiated a project in October, 2004 to implement a university wide enterprise directory and email system, based on Microsoft Active Directory 2003 and Exchange 2003. The objective is to design and configure the infrastructure to support a new enterprise directory based on Microsoft Active Directory 2003 and a consolidated email system based on Exchange 2003. The design must provide for central support of a common infrastructure with distributed management. Appropriate administrative privileges are delegated to distributed IT staff, who manage the IT resources in their individual areas of responsibility.

The selected design was a single forest, single domain model with centralized user provisioning. Organizational units are created for each singularly managed department. Although much of the functionality is centralized, the intent is to enforce shared governance over the central administration with little to no oversight of the distributed administration.

The Organizational Units are designed to follow the "Vegas" rule. What happens in an OU should have no impact on the remainder of the directory and should not be the concern of other administrators, assuming that all administrators comply with the processes and guidelines set forth in this document.

This document is organized as a reference for USC IT personnel who will use the USC Active Directory. This document is considered a "living document" and will be updated as new information is available. This document replaces the original USC Active Directory & Exchange Oversight Guide, published December, 2006. The most current version of this guide can be found at http://www.sc.edu/universityemail/. [ limit access to usc users only]
# Glossary of Terms

The following terms are used extensively throughout this document.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Organizational Unit (Area OU)</td>
<td>The area organizational unit is the highest level OU that is delegated access directly from the enterprise administrator. Examples of area organizational units are campuses, colleges, and senior administrative departments.</td>
</tr>
<tr>
<td>Area OU Administrator (Area OU Admin)</td>
<td>The administrator that is granted ownership of the area OU; that administrator must be approved by a senior manager such as a director or a dean.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>This is the unit of departmental management for the USC Active Directory.</td>
</tr>
<tr>
<td>OU Administrator (OU Admin)</td>
<td>The administrator for any OU.</td>
</tr>
<tr>
<td>Sub OU</td>
<td>Any OU that is within the tree structure of an area OU.</td>
</tr>
<tr>
<td>AD Administrator</td>
<td>Anyone who has an administrative role within AD; this is a “catch-all” term to refer to enterprise administrators, domain administrators, and all OU administrators. This term is used throughout the document to refer to this larger group.</td>
</tr>
<tr>
<td>AD Operator</td>
<td>Anyone who performs normal operational support for objects within Active Directory. Examples include managing membership of groups and managing printers. Operators do not require administrative accounts to perform their duties.</td>
</tr>
<tr>
<td>USC Active Directory &amp; Exchange Oversight Committee (AD Oversight Committee)</td>
<td>Often referred to by the shorter name “AD Oversight Committee”, this is the group that serves as a change management approval and governance body for the management of the shared Active Directory and Exchange environment. More information regarding the AD Oversight Committee can be found in Section 14 of this document.</td>
</tr>
</tbody>
</table>
## 3 Roles

The administration and operations of the USC Active Directory and Exchange E-mail system includes several key roles. The following sub-sections identify those roles and the responsibilities associated with each of these roles.

- AD Operator
- Area OU Administrator
- OU Administrator
- Domain Administrator / Enterprise Administrator
- Exchange Administrator
- Oversight Committee Member
- Executive Sponsor

<table>
<thead>
<tr>
<th>Role</th>
<th>Rights</th>
<th>Sample Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD Operator</td>
<td>Provisioned User Account – granted appropriate Permissions by OU Administrator</td>
<td>• Helpdesk functions&lt;br&gt; • Workstation Support&lt;br&gt; • Printer Management&lt;br&gt; • System Administration&lt;br&gt; • Group Membership Management&lt;br&gt; • User Assistance</td>
</tr>
<tr>
<td>OU Administrator</td>
<td>OU Admin Account</td>
<td>• OU Management&lt;br&gt; • Security Group Creation and Management&lt;br&gt; • Other Administrative Functions</td>
</tr>
<tr>
<td>Area OU Administrator</td>
<td>OU Admin Account at the top level of the organization</td>
<td>• Area OU Management&lt;br&gt; • Sub-OU Delegation&lt;br&gt; • Group Policy Management (if specified)&lt;br&gt; • Other Administration Functions</td>
</tr>
<tr>
<td>Domain Administrator</td>
<td>Domain Admin Account</td>
<td>• Domain Management&lt;br&gt; • Domain Controller Management and Administration</td>
</tr>
<tr>
<td>Enterprise Administrator</td>
<td>Enterprise Admin Account</td>
<td>• Active Directory Administration&lt;br&gt; o Day-to-Day Operations&lt;br&gt; o Capacity Planning and Management&lt;br&gt; o Problem Diagnosis and Correction&lt;br&gt; o Recommend Configuration Changes to the USC Active Directory &amp; Exchange Oversight Committee</td>
</tr>
<tr>
<td>Exchange Administrator</td>
<td>Exchange Admin Rights</td>
<td>• Exchange Server Management &amp; Administration&lt;br&gt; • Day-to-Day Operations&lt;br&gt; • Capacity Planning and Management&lt;br&gt; o Problem Diagnosis and Correction&lt;br&gt; • Recommend Configuration Changes to the USC Active Directory &amp; Exchange Oversight Committee</td>
</tr>
<tr>
<td>Executive Sponsor</td>
<td>Not Applicable</td>
<td>• Resolution of Escalated Issues</td>
</tr>
<tr>
<td>Oversight Committee</td>
<td>Not Applicable</td>
<td>• Review and Approval of Domain/Enterprise Changes.&lt;br&gt; • Conducting Periodic Operational Reviews.&lt;br&gt; • Reviewing Root Cause Analyses for Problems that May Occur.&lt;br&gt; • Recommending Changes or Additional Feature/Functions to the Existing Environment.&lt;br&gt; • Sponsoring training for the USC IT Community.&lt;br&gt; • Managing the Life Cycle for Group Policy&lt;br&gt; • Maintaining the Active Directory Reference Guide.</td>
</tr>
</tbody>
</table>
4 Organizational Unit Structure

The area (commonly known as top level) organizational units will be established with the onset of Active Directory. Organizational units may create sub-organizational units. It is expected that the OU topology will closely mimic the functional structure of the network managers. The following diagram is an example of the area OU structure. Please note as the overall structure of the University is dynamic over time, the area OU structure will change accordingly.
5 Managing the Active Directory Hierarchy

The forest and domain are managed by a staff of enterprise administrators and domain administrators within University Technology Services, according to the guidelines specified in this document. Area OU’s are defined for each campus, major administrative department, each college, and each stand-alone unit within the University. Area OU administrators may create a sub-OU hierarchy and delegate permissions, according to the guidelines specified in this document.

5.1 Responsibilities of AD Administrators

The following are the key responsibilities that an AD Administrator is expected to assume in accordance with the guidelines defined in this document.

1. An AD Administrator must abide by the standards and guidelines defined in this document.
2. An AD Administrator must use his/her administration account rather than his/her personal AD account to perform administrative duties within the USC Active Directory. Any person who is performing the duties of an AD Operator does not require an administration account.
3. An AD Administrator must abide by the standard naming convention for all objects created in the ds.sc.edu domain. These objects include Computers, Printers, Groups, Group Policies, etc. This naming standard is outlined in Section 6 of this document.
4. The AD Administrator must register the organization’s 4 character naming prefix(es) to be used in the standard naming convention.
5. The AD Administrator is prohibited from directly creating user objects via Active Directory Users and Computers (ADUC), command line tools such as DSADD.exe, or other tools which directly manipulate the Active Directory. All user accounts must be provisioned via the C60 mainframe table to avoid collisions with existing accounts and to maintain a secure Active Directory. Administrators may request employee, guest, resource, admin, and retiree accounts by placing a ticket with the UTS Help Desk until the self service web interface for requesting accounts is complete.
6. If an AD Administrator creates additional layers of hierarchy within his/her OU, and additional administrators are given rights within the OU, then the granting Administrator assumes some responsibility for compliance by the other OU Administrators to the standards and guidelines defined in this document and for their actions.
7. The AD Administrator is expected to respond to and comply with requests from the AD Oversight Committee in a reasonable timeframe. An example may be a request to delete a group policy that is no longer linked.
8. The AD Administrator must subscribe to UTS ITConnection (http://itc.sc.edu/) to ensure the AD Administrator is made aware of outages and changes to USC’s Active
Directory and Exchange systems, and can communicate such to their users.

9. The AD Administrator is expected to stay current with updates to this document.

## 5.2 Enforcing Compliance

### 5.2.1. Categories of Offenses

There are two categories of offenses, **critical** and **non-critical** offenses.

- Critical offenses are those which result in system failures, such as an application that is harvesting Active Directory data and over-running the domain controllers, or an application that is forcing undue load on the USC network. Critical offenses require immediate action. The enterprise administrator must use his/her judgment to resolve the situation as fast as possible, and then contact the appropriate administrators and inform the AD Oversight Committee after the fact. The AD Oversight Committee will request a root cause analysis (RCA) session for all critical offenses to ensure that a long-term solution is implemented so that the situation or problem will not re-occur.

- Non-critical offenses are infractions of the rules and guidelines specified in the USC Active Directory Operations Guide that do not have an immediate impact on the health of the USC Active Directory. An example of such is joining computers to the AD domain that do not comply with the naming standard.

### 5.2.2. Consequences and Escalation

The following are the consequences and escalation path for implementing a suitable long term resolution for non-compliance.

1. First Offense: For the first offense, an e-mail will be sent by the USC Active Directory Enterprise Administrator to the OU administrator (or other administrator) at the level where the offense has occurred. Members of the USC Active Directory & Exchange Oversight Committee, and the area OU administrator (if not the same person) will be copied on the e-mail. Explanation of the offense, and the recommended corrective action will be included in the e-mail. A time frame of 5 business days will be given for a non-critical offense to be corrected.

   If no response is received after 5 business days, the USC Active Directory Enterprise Administrator will send another e-mail to the same people listed above, and also to the administrator’s supervisor, co-workers, etc. in case the first e-mail was not received or the person in question is out of town or on vacation.
2. Second Offense: A second offense will include the following:
   - no response after 10 business days to the first offense e-mail, or
   - two offenses within a six month time frame.

For the second offense, a letter will be written, including the information in the first offense e-mail. This letter will be sent to the person who created the non-compliant issue, his/her supervisor, and the senior manager who signed the request form for the administrator account. In this letter, it will be stated that if the non-compliant issue is not corrected within 5 business days, then the third step will include disabling the administrator account.

1. Third Offense: A third offense will include the following:
   - no response after 10 business days to the second offense e-mail,
   - three offenses within a six month time frame.

For the third offense, the administrator account will be disabled. The Deputy CIO and CIO will be copied, in addition to everyone on the communication for the second offense, and to the administrator, informing him/her that his/her account has been disabled. The administrator in question must petition the USC AD and Exchange Oversight Committee to regain his/her administrative access via e-mail (ADOversight@sc.edu). The AD Oversight committee will be convened within 5 business days of the receipt of the e-mail request and will determine when and if the account will be re-enabled.

5.2.3. Exceptions

Situations may occur where an administrator may have to implement an application, server, workstation, etc. that may not be compliant for a temporary period of time. The administrator may petition the AD Oversight Committee via e-mail prior to the implementation to be granted a waiver. The AD Oversight Committee will respond within 5 business days of the receipt of the e-mail request.

5.3 Enterprise and Domain Administration

The forest and domain are managed by a staff of enterprise administrators and domain administrators within University Technology Services, according to the guidelines specified in this document.

Enterprise and Domain Administrators will be provisioned just like other OU Administrators. The Admin UserID will be added to the appropriate Domain Administrators or Enterprise Administrators Group in Active Directory, depending on the role the person will have. The Enterprise and Domain Administrators who work in University Technology Services Data Center Operations will be Microsoft certified with a Microsoft Certified Systems Engineer (MCSE) in Windows Server 2003.
5.4 Organizational Unit Administration

Each area OU will be managed by an area OU administrator. That area OU administrator may create sub-OUs and structure a hierarchy of organizational units beneath that area OU that best serves his/her campus, college, or department in accordance with the guidelines specified in this document.

5.4.1 Delegation of an Area OU

The actual delegation of an area OU must be requested via a ticket to the UTS Help Desk. OU administrators can do so via the following methods:
- Calling the UTS Help Desk at 777-1800
- Placing a ticket via the web interface (https://helpdesk.uts.sc.edu/)
- E-mailing the UTS Help Desk at helpdesk@sc.edu.

The requesting administrator must complete the request for administrator account form (see Appendix A); that form must be signed by a senior manager within that campus, college, or department, such as a dean or director.

The signature on the form indicates that the area OU administrator understands the procedures, rules, and guidelines defined in this document, and indicates his/her agreement to comply and to stay informed as new revisions are published.

Once the completed form is returned to UTS, the enterprise administrator will delegate ownership of the OU to the area OU administrator. This is done via group membership. A security group is given the necessary permissions at the OU level. The OU administrator is made a member of that group.

Each area OU administrator may designate a single point of contact and backup for the organizational area.

5.5 Delegation of Sub-OU’s

The area OU administrator can create sub-OUs and structure a hierarchy that best fits his/her organization. Each area OU designated point of contact must request an OU administrator account (see section 8.1.1) for each additional OU administrator within his/her organization. Each OU administrator must complete and sign the OU administrator account request form, indicating his/her agreement to comply with the procedures, rules, and guidelines defined in this document. The form must additionally be signed by the OU Administrator’s supervisor, or someone within his/her management chain, and by the area OU administrator.

The area OU administrator can then delegate ownership of sub-OUs to other administrators within his/her organization. OU’s must be delegated to the sub-OU administrator account, not to the administrator’s normal user account.

Only the security group of which the area OU administrator is a member is provided the right to create group policy by default. The area OU administrator must specify group policy rights when requesting additional OU administration accounts for any OU administrators within his/her organization that will need group policy rights. If the additional OU administrators are at the same area level, and are, therefore, members of the same area level security group, then they will have the rights to create and manage group policy.

[better wording?]
5.6 **Best Practices for Structuring an OU**

Structuring the organizational unit hierarchy for a campus, college, or department is very much dependent on the IT practices of that organization. An OU administrator can decide to restructure and move objects at a later date, but a good structure in the beginning will reduce work later on. This section contains advice on how best to approach the decision of how to partition the objects that must be managed into the most logical OU structure for the organization.

OU Administrators may want to consider the following in structuring the organizational unit hierarchy.

- If different administrators within the organization have unique areas of support, then it may be beneficial for the OU hierarchy to be structured to group objects logically to match the responsibilities and permissions of the administrators.
- Some administrators may choose to structure the OU to match group policies that will be applied to the various computers. It may be beneficial to group lab computers that will be used by students in unique OU’s and group the faculty/staff desktop computers in another OU.
- Some administrators may choose to sub-divide OU’s for clarity in management and to limit the sheer size of any individual OU. By default, Active Directory Users and Computers (ADUC) will not list more than 2,000 objects within an OU.
- The OU structure does not necessarily have to match the HR organization. A common mistake is to create too many sub-OU’s to match the logical design of the organization. The optimal OU structure is the one that best facilitates management of the objects.

The following is an example of an OU structure that combines several of these factors.

```
Academic Department
  Computers
    Faculty
    Staff
  Labs
    Lab 1
    Lab 2
    ...
    Lab N
  Servers
  Groups
    Security Groups
    Email Groups
Printers
```
6 Naming Conventions

6.1 Standard Prefix
As devices, groups, group policies, and others must have unique names within the USC Active Directory, the following convention has been adopted. Each organization will prefix these names with a standard 6 character string that identifies that organization. Organizations may have several prefixes to represent each department or each major group within the organization. All naming standard prefixes must be registered prior to use with the enterprise administrator to ensure no duplicates.

The following conventions apply
- The prefix will be 6 characters in length.
- The first 2 characters will represent the campus
  - CO – Columbia
  - CH – Charleston
  - AI – Aiken
  - UP – Upstate
  - UN – Union
  - LA – Lancaster
  - BE – Beaufort
  - SA – Salkehatchie
  - SU – Sumter
- The next 4 characters will represent either the College, Department, or Administrative Department.
- The 6 character name must be:
  - Upper case,
  - Alphanumeric characters only, and
  - Have no dashes as filler.

6.2 Registering a Standard Prefix
Before assigning names to devices, groups or others, administrators are asked to reserve the 6-character prefix by placing a support ticket with the UTS Help Desk. OU administrators can do so via the following methods:
- Calling the UTS Help Desk at 777-1800
- Placing a ticket via the web interface (https://helpdesk.uts.sc.edu/)
- E-mailing the UTS Help Desk at helpdesk@sc.edu.

The request should state your name, the prefix that you are requesting, the department or college, and what the prefix represents; i.e., “CASD” denotes the College of Arts and Sciences Desktops. Please note that although academic departments have had course names that use a standard 4-character moniker, there is still much opportunity for conflict. If you plan to use your department’s standard names for course offerings, please register this name with UTS.

If your name choice is already reserved by another OU administrator, you will be asked to select a different name.
6.3 Device Names
The following apply to workstations, servers, and printers.
- Device names should not exceed 15 characters unless the NetBIOS name is not used or required.
- In keeping with best practices to ensure usability, clarity, and ease of scripting, device names should not exceed 20 characters in length.
- The first 6 characters of the device name will be the organization’s standard prefix.
- The remaining characters are at the discretion of each organization. Dashes are allowed.

6.4 Group Names
The following apply to group names.
- In keeping with best practices to ensure usability, clarity, and ease of scripting, group names should not exceed 20 characters in length.
- The first 6 characters of the group name will be the organization’s standard prefix.

6.5 Group Policy Names
The following apply to group policy names.
- In keeping with best practices to ensure usability, clarity, and ease of scripting, names of group policies should not exceed 20 characters in length.
- The first 6 characters of the group policy name will be the organization’s standard prefix.

Group policies that are selected and offered by the Oversight Committee as available for use by any OU administrator will be prefixed with “USCGPO.”

6.6 E-Mail Distribution Lists
E-mail distribution lists follow the same group name requirements listed in section 6.4, as e-mail distribution lists are essentially groups that have been “mail enabled.”

As there are many e-mail addresses in place for distribution lists and resources that are used by numerous persons, including those outside the USC community, it is not practical to require a naming convention for the actual e-mail address that represents the distribution list. Thus, when possible, it is advised to use the 6-character standard prefix assigned to the organization to prefix the e-mail address.

When following this naming convention is not possible or practical, a unique name for the e-mail address can be used. The name must be requested and reserved with UTS Data Center Operations. E-mail address names will be reserved on a first come, first serve basis. [should a support ticket be placed.]
6.7 Requesting an E-Mail Distribution List

An OU administrator may reserve an e-mail distribution list and address by placing a support ticket with the UTS Help Desk via the following methods:

- Calling the UTS Help Desk at 777-1800
- Placing a ticket via the web interface (https://helpdesk.uts.sc.edu/)
- E-mailing the UTS Help Desk at helpdesk@sc.edu.

The request should contain the name of the group to be mail enabled. The default e-mail address will be groupname@mailbox.sc.edu. If a different e-mail address is required, then it must be submitted in the request with the appropriate justification. If the e-mail address requested does not use the standard naming convention and is already reserved, you will be asked to select a different e-mail address to use.

It is expected that the self-service web interface for OU administration will incorporate this functionality when it is available.

6.8 User Account Names

All user names are allocated by a mainframe program. User account names are limited to 8 characters in length and must be some combination of the user's first and last names. There have been numerous requests to allow longer user account names. This standard is expected to change only when the new Enterprise Resource Planning (ERP) application is implemented.

Please see section 7 for more information regarding user accounts and the various types of accounts.

6.9 Resource Account Names

As user account names are limited to 8-characters, it is not feasible to impose the 6-character standard prefix for resource accounts. Thus, resource names must be requested and reserved with UTS Data Center Operations. Resource names will be provisioned on a first come, first served basis. The process for requesting a resource account is summarized in section 7.5.
7 User Accounts and Provisioning

All User accounts are provisioned from the C60 mainframe table to ensure that there are no name conflicts and to ensure that each account is appropriately credentialed. The C60 table includes data from the Student database and the Human Resources (HR) database. The usernames are created by mainframe programs and stored in the C60 table. An interface exists to reserve usernames and record them in the C60 table. These reserved usernames are what eventually become resource accounts, admin accounts, and guest accounts.

The C60 table is updated nightly; an output file is produced that is used as input to the Active Directory provisioning application which runs each morning. Additions, deletions, and changes to accounts are performed each day, according to what is recorded in the C60 table.

Within the USC Active Directory, the following types of accounts are all InetOrgPerson objects. There is no difference between these objects other than the values of USC specific attributes.

- Student
- Employee
- Retiree
- Affiliate
- Admin
- Resource
- Guest

A self-service web interface is being developed for AD administrators to request and modify accounts. Until this interface is developed, AD administrators will have to place a ticket with UTS Help Desk via one of the following methods:
- Calling the UTS Help Desk at 777-1800
- Placing a ticket via the web interface (https://helpdesk.uts.sc.edu/)
- E-mailing the UTS Help Desk at HelpDesk@sc.edu.

7.1 Student Accounts

Student accounts are provisioned from the student database. There is no method for proactively or manually creating a student account.

A student account is created when a student application is accepted and “committed” to the university. The term “committed” actually refers to when a student record is moved from the pre-admissions database to the student database. The student’s mailbox is provisioned as well. The status of the account is inactive until the student registers for his/her first class. Although the status is technically “inactive” during this time, the student is still able to use his/her account name to log into various enterprise applications, such as Blackboard and still maintains the use of his/her mailbox, assuming he/she has set his/her network username password in VIP (https://vip.sc.edu).

Once the student registers, his/her account status changes to active. The account remains active as long as the student continues to register for courses. When he/she skips a
semester during the normal academic year, the account status changes back to inactive. Again, inactive student accounts allow logins to enterprise applications and maintain current mailboxes.

One year after the student’s last class taken, the account status changes from inactive to disabled. (Graduate students are allowed two years after the last class taken.) Once the account is disabled, the student will no longer be able to log into enterprise applications or access his/her mailbox.

Thirty days after the student account is disabled, the mailbox is deleted. One year after the account is disabled; the account is scheduled for deletion from the Active Directory. At that time, the username is no longer reserved and can be reassigned.

In the event that a student application is accepted and committed, but the student fails to register for a class, his/her Active Directory account and Exchange mailbox will remain provisioned for two years after the date the account was first created. The status will remain inactive during this time. If the student fails to register within that period, the account status is changed to disabled for 30 days, and then scheduled for deletion.

### 7.2 Employee Accounts

Employee accounts are provisioned from the HR database. Most departments require e-mail and network access for their new employees before the employee’s data can be fully processed by HR. AD administrators will be able to request employee accounts via the provisioning interface when that is complete. In the interim, OU administrators may request a pre-employee account by placing a ticket with the UTS Help Desk. This process will allow an employee account to be reserved and created before the HR paperwork is processed and the HR record entered.

Employee accounts are provisioned as active accounts; the Exchange mailbox is also created at this time. When an employee terminates, the account status changes to disabled. Once the account is disabled, the employee may no longer access enterprise applications or his/her mailbox. One year after the account is disabled, the account and mailbox are scheduled for deletion. Retaining the mailbox while the account is disabled for one year allows the department sufficient time to retain any e-mail messages which must be saved.

#### 7.2.1 Expediting an Employee Account

An AD administrator may expedite an employee account by placing a support ticket with the UTS Help Desk. A guest account will be provisioned. The future employee’s name, department code, sponsor, and social security number must be provided so that when the employee’s information is finally entered into the HR system, the account can be matched back to the employee. Once the HR record is processed and the pre-registered account is matched, the account is processed as a normal employee account.

#### 7.2.2 Adjunct Employee Accounts
Adjunct employees represent a special case as they often terminate and are then rehired within a few weeks or months. When an adjunct employee terminates, the account status changes to inactive and remains inactive for 200 days to allow the adjunct employee to retain his/her network access and mailbox. If the adjunct is not re-employed within 200 days, his/her account is then disabled. The account is then treated the same as a normal employee termination.

7.3 Retiree Accounts

When an employee retires rather than terminates, his/her account remains active until October 31st of the year in which he/she retires. This will allow sufficient time for his/her department’s AD administrator to sponsor his/her account. Sponsored retirees will retain their Active Directory account and e-mail and remain in an active status until their accounts expire. Once the sponsorship expires, the account is disabled. One year after the account is disabled, the account and mailbox are scheduled for deletion.

7.3.1 Requesting or Renewing a Retiree Account

An AD administrator may sponsor a retiree account by placing a support ticket with the UTS Help Desk. The AD Administrator must provide the retiree’s name and the network username for the retiree. When an employee retires, his/her account remains active until October 31st of that same year. The request to sponsor the account should be made prior to October 31st. If the request is not made prior to October 31st, there is no guarantee that the retiree will retain the same account or mailbox.

The expiration period will be set for 1 year. The AD administrator must renew the retiree account via the web interface or placing a ticket with the UTS Help Desk each year for the retiree account to remain active.

7.4 Affiliate Accounts

Affiliate accounts are provisioned from the HR database. Each affiliate account has an expiration or end date. The affiliate account remains active until the expiration or end date for that account. HR is responsible for reviewing affiliate accounts on a scheduled basis to ensure that only those affiliates who are still in place retain accounts and e-mail and for extending the end dates as appropriate to ensure that current affiliates do not lose access.

The account is disabled once the expiration or end date occurs. The account and mailbox remains disabled for 1 year and are then scheduled for deletion.

7.5 Admin Accounts

Admin accounts are provisioned upon request from the enterprise administrator, domain administrator, or OU administrator for the delegated departmental, college, or campus OU. When the provisioning web interface is implemented, requests will be made via that interface. In the interim, a ticket must be submitted to the UTS Help Desk.
The account request for the area OU administrator must be approved by the manager or director of the requesting department. See Section 5 of this document for further details. The requestor must complete the Request for OU Administrator Account Form found in Appendix A of this document.

The admin account is created with an expiration period of one year. The requesting AD administrator for a department is responsible for renewing all admin accounts on a yearly basis. Admin accounts remain in an active status for that year. If the admin account is not renewed when the expiration date occurs, the account is disabled. The account remains in a disabled state for an additional year; after that, it is scheduled for deletion.

As a general rule, admin accounts do not have mailboxes associated with them.

### 7.6 Resource Accounts

Resource accounts are provisioned upon request from OU administrators. When the provisioning web interface is implemented, requests will be made via that interface. In the interim, a ticket must be submitted.

The request for a Resource account must include the following information:
- Requestor name
- Proposed name
- Purpose
- Sponsor (Sponsor must be an OU admin account.)
- Home Department Code
- Whether the account should be e-mail enabled or not
  - If the resource account will be mail-enabled, a first-name and last-name as it should appear in the Exchange Global Address List (GAL).

The resource account is provisioned for a maximum duration of one year. The OU administrator is responsible for renewing all resource accounts on an annual basis. Resource accounts remain in an active status for that year. If the resource account is not renewed when the expiration date occurs, the account and mailbox (if one is associated with the account) are disabled. The account remains in a disabled state for an additional year; after that, both account and mailbox are scheduled for deletion.

Please note that the OU administrator who sponsors a resource account is ultimately responsible for that account. The use of resource accounts as “generic” accounts is highly discouraged. AD administrators are responsible for protecting the security of resource accounts.

### 7.7 Guest Accounts

Guest accounts are provisioned upon request from AD administrators. When the provisioning web interface is implemented, requests will be made via that interface. In the interim, a ticket must be submitted to the UTS Help Desk. Please note that the requesting AD administrator is considered the sponsor for that guest account and is ultimately
responsible for that account and for ensuring that the guest who will be using the account understands the USC policies that govern account usage.

The request must include a length of time that account should remain active, up to 1 year. A valid social security number should be provided for all guest accounts. Please note that the AD administrator who sponsors the account is ultimately responsible for that account while it remains active.

The guest account is provisioned with a maximum duration of one year. The sponsoring AD administrator is responsible for renewing accounts for guest who require access for a longer period of time. An AD administrator can also request early termination of a guest account that he/she is sponsoring. If a guest requires access for multiple years, the AD administrator should contact HR and request that the guest receive affiliate status.

Guest accounts remain active until they are either expired or terminated upon request of the sponsoring AD administrator. If the guest account is not renewed prior to when the expiration date occurs, the account and mailbox are disabled. The account remains in a disabled state for an additional year; after that, both account and mailbox are scheduled for deletion.

7.8 Account Management

7.8.1 Requesting a Larger Mailbox for an Employee

AD administrators are asked to encourage their users to be good stewards of USC’s resources; however, 300 MB may not be sufficient for many of our faculty members and our senior level staff. An online archival product is being procured. Once it is implemented, it is expected that the number of requests for expanded mailbox sizes will diminish.

An AD administrator may request an e-mail extension by placing a ticket with the UTS Help Desk. The username of the account will be required to process the request and the target size of the mailbox. Mailboxes will be expanded in increments of 300 MB. Senior management approval may be required for a mailbox extension.

7.8.2 Requesting a Username Change

The 8-character username is a derivative of the user’s first and last names. Some users may experience a change in marital status and do not want to continue with a username that has no association with their current name. The process for changing a username might involve several steps as the username is often propagated into enterprise applications such as Blackboard. Instructions for requesting a username change can be found at http://www.sc.edu/username.

7.8.3 Terminating or Administratively Disabling Accounts

The normal process for terminating accounts is to allow the account aging rules implemented in the provisioning system to take effect. There are times when exceptions must be implemented.
Just as in the hiring process, there is a delay from the time a person actually is terminated and the point in time when the HR system records the termination. Some departments may request that the employee’s account be disabled on the termination date. There also may be situations in which a department may request that an account be administratively disabled.

The AD administrator should place a ticket with the UTS help desk requesting an account exception and specify a date and time. The technician who processes the ticket will treat this situation with the utmost confidentiality.

### 7.8.4 Retaining E-Mail for Employees Who Have Terminated

It is not unusual that a department may need access to the mailbox of an employee who has recently terminated or retired so that key business correspondence can be retained. The requests can be made by the IT staff within the department; however, once the ticket is placed, UTS will ask for confirmation by a senior manager within the department (dean or AVP level) via an e-mail request and reply for authorization to proceed.

Once authorized, the requestor will be provided access to the mailbox for a specified amount of time, generally no longer than one week. The contents of the mailbox will be available for one year, but access will be disabled. It is the responsibility of the requesting department to determine a more permanent arrangement if the content is needed for a longer period of time.

Please note that it is not appropriate for an e-mail account associated with a terminated employee to continue to accept or send e-mail as that employee. The department may request that an auto-reply message be configured that can point correspondents to the e-mail address of a person that is now associated with the function served by the terminated employee. This auto-reply will be in place only for a specified amount of time, generally one to two months.

### 7.8.5 Continuing Accounts for Employees Who Have Terminated

Some departments may want to allow an employee who has terminated to retain access to his/her account and email. In this case, the AD administrator may request that the account be converted to a guest account. The request can be made via the web interface or by placing a ticket with the UTS Help Desk.

Please note that the AD administrator is responsible for renewing the account on an annual basis. Also, the terminated employee will no longer appear as a member of automatically provisioned departmental groups.

### 8 Groups Provisioning

The Provisioning software will address the automatic creation of groups per the requirements developed by the workgroup. This work is scheduled to complete in 2008.
Student groups will be created to facilitate resource management by the academic departments. For example, if a lab is to be reserved for Computer Science 300, then the OU administrator can configure each workstation in the lab to allow only users in the Computer Science 300 group.

Examples of automatically provisioned student groups include the following:
- All students registered at a particular campus as their home campus
- All students taking courses at a campus
- All students taking courses in a college
- All students taking courses in a department
- All students taking a particular course
- All students taking a particular course and section
- All students registered with the department who are
  - Freshmen
  - Sophomores
  - Juniors
  - Seniors
  - Graduate Students
  - Post Doc Students
- All students registered with the college who are
  - Freshmen
  - Sophomores
  - Juniors
  - Seniors
  - Graduate Students
  - Post Doc Students

Employee groups will also be automatically provisioned to reflect the top layers of the USC organization chart. Examples of automatically provisioned employee groups include:
- All employees within the University
- All employees at a particular campus
- All employees within a major division
- All employees within a college
- All employees within a department
- All faculty members within a college
- All faculty members within a department
9 Management of Groups

9.1 Types of Groups
The following are the different types of Microsoft Active Directory groups.

- **Security Groups**
  - Can be used to grant permissions.
  - Can be mail enabled and used as email distribution lists.

- **Distribution Groups**
  - Can be mail enabled and used as email distribution lists.

9.2 Group Scope
The following are the Microsoft Active Directory group scopes.

- **Universal Groups**
  - Can contain global groups from any domain in the forest.
  - Can be contained in any type of local group (Machine Local, Domain Local, Built-in Local).
  - Can be contained in other universal groups.
  - Universal Groups should not be used in the USC Active Directory (ds.sc.edu) because there is only 1 domain in the forest.

- **Global Groups**
  - Can be contained in global groups from the same domain.
  - Can be contained in domain local groups throughout the forest.
  - Can only contain users from the domain in which it is created.
  - To grant users permissions to a resource, the users should be assigned membership in a global group. The global group should be included in a local group that has been granted permissions to the resource.

- **Domain Local Group**
  - Can only be contained in local groups of machines in the same domain.
  - Can contain global groups from any domain in the forest.
  - To grant users permissions to a resource, the users should be assigned membership in a global group. The global group should be included in a local group that has been granted permissions to the resource.
9.3 Creating and Managing Groups

The method recommended by Microsoft for assigning permissions to users through groups is the following:

1. Grant permissions for resources to domain local groups.
2. Assign users to global groups.
3. Place global groups in the domain local groups to grant permissions to users.

For Example:

The folder “SharedFolder” on a file server in the domain needs to be accessed by a group of users, “SharedUsers” who need read and write access to the folder. The following are the steps that the AD administrator should follow to grant the users within “SharedUsers” the permissions to read and write files within the “SharedFolder” file.

- The AD Administrator would create a domain local group and call it PREFIXSharedFolderRW where “PREFIX” is the location and department code registered for the OU, “SharedFolder” is the name of the file share and “RW” is the rights being granted.
- Next the AD administrator would grant the domain local group the read\write permissions to “SharedFolder”.
- Now that the folder permissions are configured, the AD administrator would then create a global group and call it PREFIXSharedUsers.
- The AD administrator would then add all the appropriate users to the global group, PREFIXSharedUsers.
- The AD administrator would then place the global group PREFIXSharedUsers in the domain local group PREFIXSharedFolder-RW to complete the process.
- Any users added to the PREFIXSharedUsers group will now have read\write access to “SharedFolder”.

9.4 Mail Enabling Groups

To mail enable a group, place a ticket with the UTS Help Desk. For more information, see Sections 6.6 and 6.7 of this document. Once the group is mail-enabled, membership of that group can be managed by anyone who is delegated permissions to that group. If a security group is not used for e-mail, the scope can be a global group. Either a security group or distribution group can be mail enabled.
10 Group Policy

10.1 Overview

Group policy is used to manage users and computers within the Active Directory. Group policy can be used to implement a task. For example, group policy can be used to distribute and install a new software package to a group of lab computers. Group policy can also be used to test sample configurations as well. Group policy can be used to manage security settings, login restrictions, running scripts at start-up, scheduling computer shutdown/startup, installing software, folder redirection, and other functions.

Group policy objects reside in a special folder at the domain level and apply only to those objects targeted.

Please note that as user objects do not reside within the distributed organizational units, the primary method for implementing policies contained in the user configuration section of a group policy object is to utilize loopback policy in replace mode and apply that to the computer objects of the users to be affected.

10.2 Who can create group policy

To create and manage group policies, AD administrators are recommended to download the Group Policy Management Console from the Microsoft website. Group policy can also be created from within Active Directory Users & Computers (ADUC) using the built-in group policy editor.

An area OU administrator may create a group policy to apply to objects within his/her OU. The policy should be named in accordance with the naming conventions defined in section 6.5 of this document.

10.3 Examples of Group Policy

Many configuration settings available on a local machine can also be set using Group Policy. Group Policy allows for these setting to be applied to workstations from one source eliminating the need to configure each machine separately. Some examples of tasks that can be completed using Group Policy are desktop configuration settings, security settings, run scripts to map drives and printers, software installation and many others.

The following is an example of using Group Policy to configure Microsoft Updates on client machines:

1. Create a new Group Policy object and link it to an OU containing the machines to be configured.
2. Edit the GP and browse to “Computer Configuration\Administrative Templates\Windows Update\Configure Automatic Updates” and select Enabled.
3. Configure the desired update schedule and settings then click OK.
4. All machines in the linked OU should now get the same Windows Update settings.
10.4 Group Policy Status Setting

In the GPO Editor, the Details tab has an option at the bottom called GPO Status. If a GPO will only be applied to computers, the AD Administrator can configure the setting to "User Configuration Setting Disabled" (see the screen shot below). This should decrease the GPO processing time, since it doesn't have to look through any user settings.

A good web site for reference is: http://calnetad.berkeley.edu/documentation/technical/gpmc/.

10.5 Using Group Policy Loopback Processing

User group policy loopback processing mode is used to apply group policy to a user through policy assigned to a machine. This is needed in the ds.sc.edu Active Directory because OU administrators will not have direct access to user objects. The two most common cases which require that user configuration group policy be configured are the application of logon scripts and the securing of lab environments.
Most commonly deployed group policy settings are applied from the computer configuration side of group policy. The following are the steps required.

1. Create a new group policy and apply it to the sub-OU containing the machines in which the policy will be applied. If needed, WMI filtering can be used to select specific workstations within the OU to get the policy.

2. Select Edit and browse to “Computer Configuration\Administrative Templates\System\Group Policy\User Group Policy Loopback Processing Mode” and Enable the policy in Replace mode.

3. Browse to “Computer Configuration\Administrative Templates\System\Logon\Always wait for the network at computer startup and logon” and Enable the policy. This setting should be considered for all group policies.

4. Policy set in the User Configuration section of this group policy will be applied to all users when logging on to the workstations where this policy is applied.

5. To exempt a group of users from being affected by the loopback policy on applied machines, you must explicitly deny the “apply group policy” right on that policy for the group of users. To do this:
   a. Open the Group Policy Management Console (GPMC) and browse to the OU where the policy is linked.
   b. Click on the policy and select the delegation tab.
   c. Click the advanced tab in the bottom right corner.
   d. In the policy security settings, add the Group or user which you want to be exempt of the policy, and assign “Allow Read” and “Deny Apply Group Policy”.
   e. The group or user will now be unaffected by this loopback policy.

10.6 Maintenance of group policy

10.6.1 OU Administrators’ Responsibility

As all group policies are stored at the domain level, OU administrators are asked to use discretion in creating and managing group policies. OU administrators should periodically review their policies and ensure that they should still be in effect. For example, group policy is an excellent tool for testing a configuration change for a group of computers or for distributing a one-time software update. Once a group policy is no longer needed,

In general, OU administrators should create as few group policy objects (GPOs) as possible. Although peoples’ tendencies may be to create separate GPOs for each task, configuring a single GPO with all the required settings is the more optimal approach from a performance perspective.

An OU administrator should not link to another OU administrator’s group policy without the expressed permission of the administrator who owns the policy. For example, if the administrator for OU A would like to use the group policy that the administrator for OU B has configured for lab machines, OU administrator A must gain OU administrator B’s permission. Assuming that OU Administrator B grants that permission, he/she should agree to consult OU administrator A before making any changes to that policy going forward.
If multiple administrators are interested in linking to a particular group policy, they should petition the AD Oversight Committee to establish a shared policy.

### 10.6.2 Oversight Committee Audit

The Active Directory and Exchange Oversight Committee is responsible for periodically reviewing the group policies in effect to ensure that the sheer number of policies does not become a performance concern and to eliminate duplicate policies.

#### 10.6.2.1 Shared Policies

Shared policies are those policies that are proposed and managed by the AD Oversight Committee. These can be identified as those policies whose name begins with the prefix “USCGPO.” The Oversight Committee should check for the following policies that are no longer linked, and thus, are not used.

- The committee must decide whether to retain the policy or if it has outlived its usefulness.
- If the AD Oversight Committee decides to eliminate the policy, there should be an email communication to all OU administrators and to the netmanag listserv to that effect sent 1 week prior to the deletion.
- The AD Oversight Committee should then schedule the deletion with the Enterprise Administrator who will perform the deletion in accordance with the UTS change management process.

- **Updates to existing policies.**
  - The AD Oversight Committee will recommend a change and notify those administrators who have linked to that policy.
  - The Enterprise Administrator will then create a copy and modify the copy per the Oversight Committee’s direction.
  - OU Administrators will be encouraged to test the new policy and migrate to the new policy.
  - Once there are no links to the old policy, it can be deleted per the steps described above.

#### 10.6.2.2 Non-Shared Policies

Non-shared policies are those policies that are created and managed by OU administrators. The Oversight Committee should periodically review the existing group policies and check for the following.

- **Policies that are not linked to any organizational unit objects, and thus no longer in use.**
  - The Oversight Committee should identify those policies.
  - The enterprise administrator should contact the owner of those policies and request that the policies be deleted.
  - The OU administrator who owns the policy may comply or respond with a reason for continuing the policy.
  - If the OU administrator agrees to delete the policy, he/she should do so or request that the enterprise administrator do so.
  - In the event that there is no response within a week, and a week of escalations, the Enterprise administrator can request approval from the AD Oversight Committee to delete the policy.
- Review similar policies and evaluate whether a shared policy should be proposed.

### 10.7 Establishing a Shared Policy

The Enterprise Administrator will provide periodic reports to the AD Oversight Committee on the group policies implemented. The AD Oversight Committee is responsible for establishing shared group policies for Active Directory or Exchange. The AD Oversight Committee can either recommend that an existing policy be made a shared policy or recommend a new shared policy.

Anyone can petition the AD Oversight Committee to convert an existing group policy to a shared policy with the permission of the owner of that policy. The AD Oversight Committee may find that there are many similar policies that could be replaced with one shared policy, or multiple OU administrators may opt to link to a particular policy. In either case, the process should be as follows:

- The owner of the policy must agree to allow his/her policy to become a shared policy. If not, a copy of that policy can be proposed.
- The AD Oversight Committee will review the policy in a meeting that is open to the OU administrator community, most likely the Network Managers meeting.
- The AD Oversight Committee will decide whether to establish the policy as a shared policy. The enterprise administrator will implement the decision.
- The decision will be communicated to all OU administrators via the netmanag listserv.

### 10.8 Current Domain Policy in Effect

The password policy requiring complex passwords and a password reset every 180 days is currently in effect as a domain policy. These settings always come from the default policy and cannot be overridden by another other GPO.
11 Migrating to AD and Exchange

11.1 Manual Desktop Migration
The following are the steps to join a Microsoft Windows workstation to the domain.

1. Log on to the workstation with local administrative privileges.

2. Change the name of the workstation to meet the adopted convention. See Section 6 of this document for more information regarding naming conventions. Restart the workstation.

3. Log on again with administrative privileges.

4. Set the DNS server entries to the ds.sc.edu DNS server entries. These are 172.27.7.112 and 172.27.7.115.
   a. Go to "Start\Control Panel\Network Connections" and open the properties for your active network connection (local area connection).
   b. Scroll down to select Internet Protocol (TCP/IP) and click Properties.
   c. If the workstation is setup to obtain IP and DNS automatically through DHCP it would be best to change the distributed DNS information on the DHCP server. The DNS server address can be statically assigned here if editing the DHCP server is not an option.

5. Join the workstation to the domain ds.sc.edu.

   If this is the very first workstation you want to join, i.e. an Administrative workstation, it is not easy to use Active Directory Users and Computers to join the computer to the Domain. This utility assumes the default container location of Computers for the new workstations. You do not have rights to create computer objects in the Domain Computers Container.

   You can use the Netdom command to add workstations to the Domain. Do not create a computer object prior to using the Netdom command. It will create the object when it runs. To get the Netdom command, use the Windows server 2003 CD and install the support tools. These are located at CD\Support\Tools\Suptools.msi. One of these tools is Netdom. Use netdom to join your administrative workstation to the domain first.

   The command syntax is similar to the following example: (Remember to rename the workstation to the correct name based on the USC Naming convention prior to running this command.)

   C:\Utilities>netdom join COCASW71566hr3xx41 /Domain:ds.sc.edu /OU:ou=staff,ou=desktops,ou=uts,ou=columbia,dc=ds,dc=sc,dc=edu /userd:vicki /passwordd:XXXXXXXX /userO:mathisv /passwordO:XXXXXXXX

   Once the machine is in the domain, login to the domain as the OU Admin. You can install Active Directory Users and Computers and other utilities from the same Windows server 2003 CD at this location, CD\i386\adminpak.msi. You should do this
on your Administrative workstation, but you do not have to install these tools on any other workstation.

11.2 Joining Macintosh Computers to AD
Macintosh computers can be joined to the USC Active Directory and authenticate users at login. Note that, by default, group policies cannot be applied to Macintosh computers.

Rename the computer to comply with the naming standards defined in section 6 of this document.

1. Browse to "System Preferences\Network" and specify the DS.SC.EDU DNS servers 172.27.7.115 and 172.27.7.112
2. Browse to "Applications\Utilities\Directory Access" and unlock the window.
3. Select Active Directory and the click the configure button.
4. Set DS.SC.EDU for the Forest and Domain. Then specify the computer ID for the machine you are binding.
5. Click Bind, and specify a username and password with rights to join computers to DS.SC.EDU.
6. For "Computer OU," Specify the distinguished name of the OU in which the username and password combination has rights to create computer accounts. If the joining account does not have machine account creation rights, the machine account will need to be populated by the proper OU Admin in DS.SC.EDU before performing a bind.
7. Click OK to finish the bind.

11.3 Server Migration
The following are the steps that AD administrators should follow in migrating from a Novell Netware file server to a Microsoft Windows file server within the USC Active Directory.

- Server Preparation
  - Prepare a new or repurposed server by installing Windows Server 2003, critical updates, antivirus software, backup software, etc.
  - Join the Windows server to DS.SC.EDU. Prepare the new system to provide the same services as the system being replaced (setup file shares, printers, securities, and other needed services).
  - Prepare and test Microsoft scripts that will provide drive and printer mappings to the shared drives and printer objects. These scripts will be deployed to users using group policy applied to workstations in loopback processing mode. Ideally the new scripts should mirror drive and printer mappings from the old system to limit user confusion.

- Workstation Configuration
Configure each workstation to authenticate with both directories (e-directory and AD). This means each machine will have the latest Novell Client (4.91 sp4) installed as well as be a member of the DS.SC.EDU domain.

- **Migration Sequence for a shared directory**
  - Complete server and workstation preparation.
  - Break down items to be migrated into manageable pieces (everything doesn’t have to be migrated at the same time because clients are configured to access both systems seamlessly.)
  - Be sure that the new Shard directory is properly configured and securities are in place before beginning a migration.
  - Use groups to configure permissions.
  - Inform users that during the migration there will be a window of time where they will not have access to their files.
  - Remark out the line in the Novell script that is giving users the current mapping that is to be migrated then implement the new script, mapping the same drive to the new share location.
  - Deny access to the source directory on the Novell server to make sure no changes can be made to the files to be migrated.
  - Copy the files to the new destination Windows server. Users should already be accessing these new locations so they should start gaining access to their files as they are migrated.
  - Repeat these steps until all directories have been migrated.

### 11.4 *Departmental Application Migration*

Applications which authenticate via LDAP to the Novell e-Directory must be reconfigured to authenticate to the USC Active Directory.

### 11.5 *E-Mail Migration*

The project team will be working with each department to migrate the departmental e-mail system into the University E-mail system. The following is a summary of what components migrate.

#### 11.5.1 Migration from GroupWise

The following is a list of each function or feature and an explanation of what to expect from the migration.

- **Mail Messages** – All messages migrate with the exception of the Trash and the Junk Mail folders.
- **Calendar Items & Notes** – All calendar items migrate; however, recurring calendar items are stored as multiple appointments. Note that notes migrate as all day events on your calendar.
- **Alarms** – will not typically migrate; however, alarms associated with appointments do migrate.
- Personal Address Book and Frequent Contacts – All contacts and personal address lists that are saved in personal address books migrate. Frequent Contacts, which are typically automatically stored whenever a user sends or receives an e-mail, are not migrated. Please note that personal address lists probably contain the internal GroupWise address for GroupWise users and must be recreated.

- Tasks – All tasks migrate.

- Rules – Rules do not migrate; the user will have to configure any rules to be retained in his/her e-mail client. Please note that configuring a vacation rule to reply to e-mails received while out of the office is no longer necessary.

- Proxies – Proxies do not migrate; users may grant access to their mailbox or calendar by configuring delegates.

- Archives – do migrate, but must be done on an appointment basis. Departmental Resource Names and E-Mail Groups – may migrate in tact; however, the resource names and groups may need to be re-created with different names to comply with the naming conventions as specified in Section 6 of this document.

In an effort to ease this transition, a Connector/GateWay that bridges the address book and the calendars between GroupWise and Exchange has been implemented for the duration of the migration. Although this bridge cannot make everything between the two systems transparent, it should assist communications during the transition.

- The address book in Exchange has an entry for all GroupWise users that point to their GroupWise mailbox. Exchange users can identify a GroupWise user in the Exchange address book as his/her name appears in lower case with the first letter capitalized. There is also an icon that resembles a globe by their names. Exchange users may use this address to send GroupWise users e-mail messages or calendar appointments.

- Exchange users may send GroupWise users calendar appointments, although busy search between the two environments is not supported. Please note that once a calendar appointment is sent, the sender will not be able to resend the appointment and have GroupWise automatically cancel or update the old appointment.

- The address book in GroupWise will have entries that point to all migrated users’ Exchange mailbox. GroupWise users will be able to send Exchange users e-mail and calendar appointments as well without having to know that they have migrated and are now using Outlook and Exchange.

- GroupWise users who receive e-mail via IMAP may receive messages from native Exchange users with unrecognizable reply-to addresses. This is an unintended consequence of the Connector/GateWay. The work-around for this problem is to replace the right-hand side of the reply-to address with “@mailbox.sc.edu.” The IMAP user may find that it is more convenient simply to migrate to Exchange. IMAP users may request that their accounts be migrated by placing a ticket with the UTS Help Desk.

11.5.1 Migration from Exchange

Users of departmental Exchange systems should experience few problems with migration to the University E-mail system. Microsoft provides tools to migrate e-mail accounts from one
Exchange system to another. The actual steps will be included in this document in a later revision.

[still need to add content here]

11.5.1 Migration from Other E-Mail Systems
The migration from e-mail systems other than Novell GroupWise or Microsoft Exchange is still to be determined. Please note that IMAP users will have little difficulty in migrating their e-mail from their current system to the University E-Mail System.
12 Data Access

12.1 HR Data
AD administrators who need access to employee data must contact Human Resources and complete a request for HR data form. This form does require management signature.

12.2 Student Data
AD administrators who need access to student data must complete a request for student data form available through the Registrar’s office. This form does require management signature. Please note that this requirement applies to any AD administrator who must manage group memberships that include students who have requested that their directory information not be published.

The Family! Educational Rights and Privacy Act (FERPA) guarantees that directory data will not be published for those students who have requested via the Registrar’s Office that their directory information be maintained private.
13 Administrative Tasks and Oversight

The following sections outline the tasks that should be performed by OU administrators and the tasks that will be performed by the domain and Exchange administrators.

13.1 OU Administration Tasks – Operational
(No Reporting, No Oversight Approval)

<table>
<thead>
<tr>
<th>Task</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC (Moves, Adds, Changes)</td>
<td></td>
</tr>
<tr>
<td>• Desktop Computers</td>
<td></td>
</tr>
<tr>
<td>• Printers</td>
<td></td>
</tr>
<tr>
<td>• Shares</td>
<td></td>
</tr>
<tr>
<td>• Group Policy</td>
<td></td>
</tr>
<tr>
<td>• Groups</td>
<td></td>
</tr>
<tr>
<td>Group Maintenance</td>
<td></td>
</tr>
<tr>
<td>Group Modifications</td>
<td>Web-based interface</td>
</tr>
<tr>
<td>Non-Area OU creation, i.e. sub OUs</td>
<td></td>
</tr>
<tr>
<td>Sub OU level login scripts</td>
<td></td>
</tr>
<tr>
<td>Delegation of OU Administration Responsibilities</td>
<td>Web based interface – Reporting built-in</td>
</tr>
<tr>
<td>Request creation, deletion of sub OU accounts</td>
<td></td>
</tr>
</tbody>
</table>

13.2 OU Administration Tasks – Reporting Requested
(No Approval Required)

<table>
<thead>
<tr>
<th>Task</th>
<th>Method/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member Server Installation &amp; Update</td>
<td>TBD</td>
</tr>
<tr>
<td>Applications that are going to impact AD</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>(need to define what goes against AD)</td>
</tr>
</tbody>
</table>

13.3 OU Administration Tasks -
Oversight Approval Required

By design, there are no OU administration tasks that require AD Oversight Committee approval. AD administrators are asked to request exceptions of the AD Oversight Committee for any situations that will violate the guidelines and practices defined in this document.
13.4 Enterprise Administration Tasks – Operational  
(No Reporting, No Oversight Approval)

UTS will perform normal operational tasks in managing the Active Directory domain controllers and the Exchange servers such as maintaining anti-virus updates, running daily backups and others with no oversight activities.

13.5 Enterprise Administration Tasks – Reporting Required

These tasks apply to the USC Active Directory and Exchange infrastructure managed by UTS.

<table>
<thead>
<tr>
<th>Task</th>
<th>Method/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Updates &amp; Server patches</td>
<td>Via ITConnection</td>
</tr>
<tr>
<td>Capacity and Performance Reporting</td>
<td>TBD</td>
</tr>
<tr>
<td>Hardware and Storage Upgrades</td>
<td>Via ITConnection</td>
</tr>
<tr>
<td>Migration plan from current environment per dept</td>
<td>Project Activities</td>
</tr>
<tr>
<td>Changes to the area OU Structure</td>
<td>Via ITConnection</td>
</tr>
</tbody>
</table>

13.6 Enterprise Administration Tasks – AD/Exchange Oversight Approval Required

These tasks apply to the USC Active Directory and Exchange infrastructure managed by UTS.

<table>
<thead>
<tr>
<th>Task</th>
<th>Method/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coding Changes to the Provisioning Software</td>
<td></td>
</tr>
<tr>
<td>Enterprise server-based software firewalls</td>
<td></td>
</tr>
<tr>
<td>Schema Changes</td>
<td></td>
</tr>
<tr>
<td>Application installs that modify or extend the schema</td>
<td></td>
</tr>
<tr>
<td>Object class creation or modification</td>
<td></td>
</tr>
<tr>
<td>Attribute Changes (additional attributes)</td>
<td></td>
</tr>
<tr>
<td>Scripted AD events</td>
<td></td>
</tr>
<tr>
<td>Policy Recommendations</td>
<td></td>
</tr>
<tr>
<td>Domain controller add / remove / modify</td>
<td></td>
</tr>
<tr>
<td>DNS server add / remove / modify</td>
<td></td>
</tr>
<tr>
<td>DHCP server add / remove / modify</td>
<td></td>
</tr>
<tr>
<td>Exchange servers</td>
<td></td>
</tr>
<tr>
<td>Mail store add / remove / modify</td>
<td></td>
</tr>
<tr>
<td>Connector add / remove / modify</td>
<td></td>
</tr>
<tr>
<td>Service Packs on DC’s and Exchange servers</td>
<td></td>
</tr>
<tr>
<td>Anti-spam configuration changes</td>
<td>Default tolerance levels – quarantine settings</td>
</tr>
<tr>
<td>Anti-virus content filtering configuration changes</td>
<td></td>
</tr>
</tbody>
</table>
14 USC Active Directory & Exchange Oversight Committee

14.1 Scope of Responsibility

The USC Active Directory & Exchange Oversight Committee (AD Oversight Committee) is charged with the responsibility for managing configuration changes to the USC enterprise Active Directory and Exchange implementation. The committee is charged with the following responsibilities:

a. Review and approval of planned changes described in the previous section of this document.
b. Conducting periodic operational reviews.
c. Reviewing root cause analyses for problems that occur.
d. Recommending changes or additional feature/functions to the existing environment.
e. Sponsoring training for the network/management committee.
f. Maintaining the AD Operations Guide.

14.2 Authority

The Active Directory & Exchange Oversight Committee is authorized by the USC Office of Information Technology to guide the evolution and operations of the university wide Active Directory and Exchange implementation.

14.3 Membership

A. Representation

The committee will consist of 7 members.

- 1 – UTS Enterprise Administrator (chair)
- 1 – UTS ITSM Representative
- 5 – Representatives elected by the Network Managers, 2 of which must be OU Administrators, at least 1 of which must be from a non-Columbia campus

Each member will designate one alternate to serve as his/her proxy when the member can not attend a meeting. The proxy should be knowledgeable of the ongoing issues and prior decisions. Five members (or their proxies) are required to participate in any vote for a quorum. The UTS enterprise administrator will chair the committee.

B. Term

The length of the term that each representative from the non-Columbia campuses and network management community shall serve on the USC Active Directory & Exchange Oversight Committee is two (2) years. The initial committee will include at least 2
members who will serve a 1-year term to ensure that the entire elected membership does not change in the same year. There is no limit to the number of terms the same representative can serve on the committee.

If a member misses 3 regularly scheduled committee meetings in a row, that member should be replaced.

C. Selection

The Oversight Committee will propose a slate of candidates for the rotating positions. The network managers will vote on the slate. The network managers forum may choose to nominate additional candidates as well. The Operations Working group will propose the initial slate.

D. Current Membership

The current membership of the Oversight Committee may be found at https://sc.edu/universityemail

14.4 Decision Process

A. Quorum

Five (5) members of the USC Active Directory & Exchange Oversight Committee or their proxies must be present and constitute a quorum. A majority Vote of the members (or proxies) is required for approval of any decision by the USC Active Directory & Exchange Oversight Committee.

B. Voting Rights

Only authorized representatives as set forth above shall be entitled to vote on proposals submitted to the USC Active Directory & Exchange Oversight Committee.

14.5 Meeting Schedule

Meetings will be conducted on a regular schedule. Using teleconferences or web meeting forums is preferable over face-to-face meetings. Ad hoc committee meetings may be called for emergency changes. The committee will meet on a regular schedule and may opt to skip any meeting for which there are no agenda items. The meetings should be open to the USC IT community, but the chairman reserves the right to limit the discussion time on any topic.

14.6 Request Submission & Approval Process

Submissions for configuration changes must be submitted to the USC Active Directory & Exchange Oversight Committee (ADOversight@sc.edu) a week prior to the meeting. Exceptions will be made for emergency situations only. Submissions should include the following information:
• Description of the change
• Impact Assessment
  o Cost (If any)
  o Risk Analysis of the Change
  o Resources Required
  o Disaster Recovery
  o Backup Plans
  o Storage Needs
  o Security Impact

• Technical References
• Tentative Schedule
• Test Plan
• Backout Plan
• Monitoring Plan

The committee is responsible for technically reviewing the change request prior to the meeting. It is best that the committee members contact the requestor with any questions prior to the meeting.

Once the change is approved by the committee, University Technology Services will schedule the change through the UTS change management process.

14.7 Incident / Problem Management Process

University Technology Services is expected to resolve any incident that occurs with the centralized system immediately. Incidents will be reported as break/fix outages in ITConnection. Incidents may include:

• Performance Issues
• Application Conflicts
• System Outages
• And others

The committee will review any incident that occurs at the next meeting and may request a root cause analysis be performed for any problem. The root cause analysis will be performed using the standard UTS process for root cause analyses and should be made available at the next regularly scheduled Oversight Committee meeting.

Any member of the user community can request that a root cause analysis be performed for any event; that request should be addressed to the AD Oversight Committee. Note that root cause analysis reports will focus on the actions to prevent further recurrence of the problem rather than the blame.

Incidents which occur solely on OU systems will not be reviewed by the AD Oversight Committee unless there is an obvious impact to the greater community.

14.8 Appeals

Any member of the IT community can file an appeal with the AD Oversight Committee in the event that the person deems that the decisions by the AD Oversight Committee were in error. The appeal should state the specific issue, the desired resolution, and the impact to existing systems or user community.
The AD Oversight Committee should initially review the submitted appeal; if the AD Oversight Committee concurs, the AD Oversight Committee can overturn its own decision. If the AD Oversight Committee decides to maintain the initial decision, the appeal will be escalated to the University Chief Information Officer (CIO) for resolution. The AD Oversight Committee will abide by the CIO’s decision.

14.9 Committee Audit

The USC Active Directory & Exchange Oversight Committee and Network Management community will establish a subcommittee to review, at least every two years, the operating and the decision making authorities set forth herein and make recommendations for improving the efficiency and effectiveness of this body. Recommendations are to be submitted to the full USC Active Directory & Exchange Oversight Committee and require a quorum and majority vote as set forth above for adoption.
15 User Support

15.1 Available Information
The University E-Mail and Active Directory Information Center provides many answers to frequently asked questions. Users are encouraged to check http://sc.edu/universityemail for general information regarding the use of either the University E-Mail System or the USC Active Directory.

Please note that during the course of the project, Outlook training will be provided to faculty/staff. Online registration is available at: http://www.sc.edu/universityemail/outlooktraining/.

15.2 Password Resets
Users may reset their passwords via VIP (https://vip.sc.edu). The steps for resetting a user's password on VIP are as follows:

1. Login to VIP (https://vip.sc.edu)
   Students who have forgotten their PIN should contact the Registrar's Office; faculty/staff who have forgotten their PIN should contact their departmental Human Resources representative.
2. Select the "Technology" Link
3. Select "Show Me Network Username"
4. Your USC Network Username will be displayed and you will be prompted to choose a password. You will be asked to type it twice for verification. Your password must be a "strong" password. Rules on legal passwords will be displayed.
5. Click on the "SET PASSWORD" button to set your password to what you have specified.

Passwords must be at least 8 characters in length. A user's password may not include any part of his/her name or username. The password must contain at least 3 of any of the following:
- Numerical symbol
- Special Characters
- Upper Case Letters
- Lower Case Letters

15.3 Shared Support Model
Many academic and administrative units maintain their own help or support desk for students and staff. There will be times when a support task will have to be routed to the UTS Help Desk, and there will also be calls which come to the UTS Help Desk that will need to be routed to the departmental help desk.
UTS has established an incident management process. The process currently utilizes the Pinnacle trouble ticket system but there is no expectation that AD administrators will adopt Pinnacle directly for departmental use.

The UTS Help Desk number, 777-1800, will be the advertised avenue for service and support. The long-term goal is to have a web-based workflow system that can allow UTS and the campuses, colleges, and departments to share the service/support workflow. In the interim, we must implement a manual system outlined as follows.

- Each department will maintain a queue for problem tickets.
- Short-term the queue will be implemented via an email address. Departments simply communicate between the departmental help desks and the UTS Help Desk via email.
- The queue ultimately needs to be a shared, automated system.

The organization that ultimately owns the resolution of a problem is responsible for following up with the customer to ensure that the customer is aware that the problem is resolved and that the customer is satisfied.

- Example – UTS Help Desk takes a call from an engineering student that must be resolved by the College of Engineering and Computing.
  - The UTS Help Desk agent identifies the caller as a student.
  - The UTS Help Desk agent opens a Pinnacle ticket to document the call.
  - The UTS Help Desk agent sends an email to Engineering’s support email alias with a copy of the information cut and pasted from Pinnacle.
  - The UTS Help Desk agent then closes the ticket.
  - The College of Engineering & Computing Help Desk addresses the problem and provides a resolution.
  - The College of Engineering & Computing Help Desk contacts the student to communicate the resolution and close the problem with the student.

- Example – College of Arts and Sciences (CAS) student or faculty member contacts the CAS Help Desk about problems with Blackboard
  - CAS agent will diagnose the problem and check for valid username, password and ensure that Blackboard is running.
  - Once the CAS agent has determined that the problem appears to be with the Blackboard system, the CAS agent will transfer the problem to UTS. The CAS agent will contact the UTS Help Desk via submitting a ticket, calling 777-1800, or emailing helpdesk@sc.edu
  - The UTS Help Desk agent will assign a ticket number to the problem and assign the problem to the appropriate UTS department.
  - The ticket number is available to the CAS agent via the web interface https://helpdesk.uts.sc.edu
  - The UTS department will assign a technician to resolve the problem.
  - The UTS technician will contact the student or faculty member if further information is required.
  - The UTS technician will resolve the problem and contact the student or faculty member to communicate the resolution.
  - The UTS technician will close the ticket.
## System Configuration Defaults

The following represents the default configurations and settings for Active Directory and Exchange.

<table>
<thead>
<tr>
<th>Configuration Default</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords must be at least 8 characters in length and must contain 3 of the following 4: Upper Case Letters, Lower Case Letters, Digits, Special Characters</td>
<td>Additionally, the password cannot contain portions of the username or name.</td>
</tr>
<tr>
<td>Passwords must be reset every 180 Days.</td>
<td></td>
</tr>
<tr>
<td>Password History is Set to 10.</td>
<td>Users can not re-use a password that was set the last 9 times.</td>
</tr>
<tr>
<td>User Account Lockout for 30 minutes after 7 failed tries within 30 minutes.</td>
<td></td>
</tr>
<tr>
<td>Student Email is Outlook Web Access <a href="https://webmail.sc.edu">https://webmail.sc.edu</a></td>
<td>Secure IMAP clients or Outlook can also be configured.</td>
</tr>
<tr>
<td>Automatic deletion of emails in the inbox folder after 60 days</td>
<td>Student email messages in the inbox folder will be deleted after 60 days. If the student wishes to retain a message longer than 60 days, he/she should move it to another mailbox folder.</td>
</tr>
<tr>
<td>Student mailboxes are limited to 50 MB in size</td>
<td>Warnings are issued automatically by the email system when space reaches 90%, 95%, and over capacity. Sending of mail is disabled until the mailbox size is brought back into compliance.</td>
</tr>
<tr>
<td>Faculty / staff mailboxes are limited to 300 MB in size</td>
<td>Warnings are issued automatically by the email system when space reaches 90%, 95%, and over capacity. Sending of mail is disabled until the mailbox size is brought back into compliance.</td>
</tr>
<tr>
<td>Outlook will be supported via RPC/HTTPS only.</td>
<td>Requires Windows XP SP2. Outlook can be configured as a secure IMAP client as well.</td>
</tr>
<tr>
<td>The fully functional Entourage client is supported as a secure WebDAV client.</td>
<td>Entourage can be configured as a secure IMAP client as well.</td>
</tr>
<tr>
<td>The daily backups for Exchange are for disaster recovery only.</td>
<td>Note that deleted emails are retained for 30 days after they are deleted from the user’s trash.</td>
</tr>
</tbody>
</table>
17 References

The following are the key documents, policies, and processes that are relevant to the operations of the USC Active Directory & Exchange E-mail system.

- USC Active Directory and Exchange Design Overview
- USC IT Policy 1.06
- University Technology Services Change Management Process
- University Technology Services Root Cause Analysis Process
- USC E-Mail and Active Directory Information Center
  [add links]
Appendix A

Request for Administrator Account
University of South Carolina Active Directory

Please complete this form with appropriate signatures and return to the UTS Help Desk for processing. Additional copies of this form may be found at http://sc.edu/universityemail/forms.

Name: ______________________________________________________________________
Preferred UserID: ___________________ Admin UserID (requested): ________________
Work Phone number: ________________ Cell Phone number: ______________________
Campus: __________________________ Building and Office Number: ________________
Department / College: _________________________________________________________

Type of Account Requested (please check appropriate box)
☐ OU Admin  ☐ Area OU Admin  ☐ Domain Admin  ☐ Enterprise Admin

Name of your Area OU (if applicable) _____________________________________________
Name and location of OU to be accessed:__________________________________________
Specific Rights to OU other than default full rights:
☐ Create & Manage Group Policy ☐ Other (Please specify) ____________________________

Unique 6 character prefix(es) for naming convention: ________________________________
____________________________________________________________________________

(This code(s) will also need to be registered as outlined in the OU Admin Operations Guide.)

Signature: ___________________________ Date: ___________________
This signature designates you have read and understand the USC Active Directory Operations Guide, and will abide by the rules outlined in the guide.

Approval (Department Chair, Dean, Director, or other Senior Management):
Name: ______________________________________________________________________
Title: ______________________________________________________________________
Signature: ___________________________ Date: ___________________

Area OU Admin Approval (for OU Admin accounts)
Area OU Admin Name: ___________________________________________________________
Area OU Admin Signature: __________________________________________ Date: __________

Does this new OU Admin work for you or in your line of supervision? ☐ Yes  ☐ No

Note: By signing this form, the Area OU Administrator accepts some responsibility for this new OU Administrator’s actions in the USC Active Directory. If this person does not work for or with the Area OU Administrator, then consideration will be granted in the case of non-compliance with the rules outlined in the USC Active Directory Operations Guide.