Active Directory (AD) Access & Control Procedures: User Accounts
(Life Cycle Management of UNMC Domain AD User Accounts)

Basis for Procedure

UNMC Policy/Procedure Link
6051 Computer Use and Electronic Information Security Policy

1. Purpose

The purpose for the Active Directory Access and Control procedure is to delineate administrative boundaries for work being done within the UNMC Domain Microsoft Active Directory environment.

The Access Control for Information Technology Resources security procedures define the system administrators as the individuals responsible for the hardware and operating systems and application software. The system administrator for Active Directory is ITS Technical Services.

The Access Control for Information Technology Resources security procedures define the information custodians as the individuals responsible for specifying the security properties of their systems. This responsibility includes ensuring that documented access control procedures are developed, maintained and followed. System Access serves as the Information Custodian of the Active Directory User Accounts.

This procedure documents the life cycle management of user accounts. The procedure relating to life cycle management of computer accounts is Active Directory Access and Control: Computer accounts

2. Definition

Active Directory (AD) is the repository for all network user and computer accounts and domain level securities. Within AD there are two account objects:

- **User Accounts**: Represents an individual or a role-specific individual.
- **Computer Accounts**: Represents a physical object such as a computer.

Server/Application Service Accounts: A server/application service account is an AD user account that is created explicitly to provide a security context for services running within the AD managed environment. Categories include:

- **Workstation Service Accounts**: A workstation service account is an AD user account that is created explicitly to allow a particular workstation access to the network. These accounts are NOT allowed to access any AD secured resources.
- **Vendor Service Accounts**: Vendors who need access to a server managed within the AD environment.
- **Test Accounts**: AD accounts created for purposes of testing within the AD infrastructure.
AD Operators: Individuals with elevated privileges within AD. (Elevated privileges would include the ability to reset passwords, and other administrative functions)

Group Policy Objects (GPO): A collection of settings that define what a system will look like and how it will behave for a defined group of AD objects. A GPO defines registry-based policies, security options, software installation and maintenance options, scripts options and folder redirection options.

Enterprise GPO’s: A collection of settings that are applied at the unmc.medforest.org or Department OU level.

3. Procedure

3.1. General
1) The AD structure is depicted in Exhibit A.
2) All AD operators are required to sign the ITS Addendum annually.
3) AD accounts in the UNMC Domain are created with rights and permissions granted to various servers, folders, and departmental shares based upon the need to access the information in order to perform job functions.
4) All UNMC faculty (except Emeritus), staff and students must have an AD account.
5) An AD account will not be created for individuals who are not faculty, staff or students without the appropriate agreements in place. It is up to the requestor of the account to contact ITS when that person has been terminated or their contract has ended.
6) The following naming convention will be used when user accounts are created:
   a) Faculty, staff and students: First name.last name
   b) Non-employee accounts: First name.last name
   c) Workstation Service Accounts ado_xxxx (description identifying specific workstation; example ado_COPHTRAIN1
   d) Appendix B identifies the algorithm used if the name of the individual would result in a duplicate ID being created.
7) The same user name CANNOT be created across the medforest.org domains (Olympus, UNMC, UNMC Physicians). There will be no duplicate usernames across any medforest.org domain.
8) User names will not normally be reused (unless it is the same person who separated and then comes back). The normal process is that the reuse will only occur when the first name.last name is utilized. In certain circumstances as determined by ITS Management, the former naming convention account may be used.
9) Annually, System Access will audit the accounts within AD to ensure that all accounts still meet the account issuing criteria.
10) An automated script runs nightly which updates identified demographic data elements in the AD based upon changes within the Human Resource System or Student Information System.
11) Enterprise GPO’s are added in order to support administrative policy. All Enterprise GPO changes are communicated to the AD operators in advance in order to ensure that there are no surprises or unexpected adverse consequence.
12) Enterprise GPO’s which are applied to user accounts are listed in Exhibit C.
13) It is acceptable for user accounts to be set up with local administrator privileges.

3.2. ITS System Access

Individuals in this group are designated by the Associate Director, ITS Operations
This group serves as Information Custodian for Active Directory User Accounts

Account Creation for Faculty and Staff:
All faculty and staff of UNMC will have UNMC domain user accounts created by an automated script. A new faculty/staff account will not show up in AD until all
necessary data required to create the account has been made available from the nightly interface with the Human Resource System. Faculty and staff accounts are not to be created outside of the automated process.

User id/passwords are distributed via an automatic notification which is an email to the department PAF coordinator and AD operator.

**Account Creation for Students:**

All registered students of a UNMC program will have an UNMC domain user account created by an automated script. A new student account will not show up in AD until all necessary data required to create the account has been made available from the nightly interface with Student Information system. Student accounts are not to be created outside of the automated process.

User id/passwords are distributed via automatic email notification which is an email to the department PAF coordinator and AD operator.

**Account Creation for those who are not faculty/staff/student (Affiliates):**

Non-employee accounts such as vendor accounts, temporary staff, and travelers will be created solely by System Access. Request form is located under the Management Resources Page, ITS, Affiliate Account Request.

User id/passwords are distributed via automated email notification to the respective college.

**Account Creation for Workstation Service Accounts:**

Workstation Service Accounts such as accounts for training rooms will be created solely by System Access. Request form located under Management Resources Page, ITS, Workstation Service Account Request. Only System Access can set up Workstation Service Accounts. With the permission of Access Services an AD Operator may rename a Workstation Service account.

User id/passwords are distributed via email communication to the requestor.

**Granting/Changing Security Access:**

When a user account needs to be moved from one OU to another, a request from the AD operator will be sent to System Access which will process the request within 24 hours.

**Name Changes:**

System Access will process name changes upon request and verification that the legal name has been changed in the Human Resource System or Student Information system

**Unlocking of AD accounts:** Follows the same guidelines as Help Desk. See below.

**Resetting AD passwords:** Follows the same guidelines as Help Desk. See below.

**Separating Access of Faculty and Staff (Disabling/deleting accounts)**

For the purpose of AD, there are 2 types of separations that occur.

**Type 1:** The Human Resource System separation date causes the user account to appear on a separation list. The account is disabled the day following separation with deletion 30 days following.

**Type 2:** Special Circumstances (Emergency Removal of Access)
**Terminating Access for Students:**
Student access is disabled based upon the following schedule:
- Spring/Summer graduates: October
- Winter graduates: March

30 days following the account being disabled the account is deleted. Many students return to the organization following graduation by enrolling in another program or becoming employed by the organization. Access is disabled with this schedule in order to provide continuity of the education environment.

Students who are on a Leave of Absence may retain their AD account. Students who are not actively enrolled in a UNMC program may have a one semester extension with the approval of Academic Affairs. This extension is normally granted to students who have taken an incomplete in a class and are completing the course work.

**Enabling a Disabled Account:**
Only the individual who disabled the account may enable the account. Accounts are only enabled when appropriate approval is obtained.

### 3.3. ITS Technical Services

Individuals in this group are designated by the Associate Director, Technical Services. This group serves as System Administrators for Active Directory. They serve as the second line of support on user account functions related to Active Directory.

**Adding Enterprise Group Policies:**
Upon request and review, the Group Policies are placed and implemented by Technical Services. A change request will be entered into the Change Management System. Upon approval from the Change Advisory Board (CAB), the change will be implemented.

**Granting/Changing Security Access:**
Upon request and review, Technical Services will change security parameters of AD Operators. Technical Services is the only area which can change the security parameters of AD Operators.

**Adding Server/Application Service Accounts:**
Technical Services will establish a server/application service account. Technical Services personnel will ensure that the appropriate security is established. The Information Security Officer is available to review unique circumstances.

User id/passwords are distributed via two emails sent to the requestor. Emails will be sent only to unmc.edu addresses.

**Disabling Accounts:**
In the situation where the AD or email is at risk due to a compromised AD account, the AD administrator may disable an account. In this situation, the AD administrator shall place a comment in the AD Description field indicating that the account was disabled, by whom and when. In addition, the AD administrator shall notify Operations.

**Second line of support**
ITS Technical Services will perform the following as a second line of support to AD Operators and will follow the same guidelines as defined below:

**Granting/Changing Security Access:**
Disabling Accounts
Enabling a Disabled Account:
Unlocking of AD accounts:
Resetting AD passwords:

3.4. AD Operators

Individuals in this group are designated by the Associate Director, ITS Operations. This group includes the individuals who work directly for the Colleges and are referred to as “independents”.

Granting/Changing Security Access:
Resource access is controlled by a user’s group membership. While coordinating with the user’s administration/management, the user is added to the appropriate AD Groups. If there is a change of job function as identified by the user's administration/management, the AD Operator will coordinate the transfer of group membership and therefore access. If an OU change is required, AD Operators will request System Access to make the OU change.

Unlocking of AD accounts: Follows the same guidelines as Help Desk.
Resetting AD passwords: Follows the same guidelines as Help Desk.

Adding GPO's
AD Operators develop/test group policies which are then implemented by Tech Services. Group policies are utilized such that the user login experience is consistent no matter what workstation is utilized.

In the event that the GPO is an Enterprise GPO, the Manager of Customer Support will facilitate communication to the AD Operator group.

3.5. Help Desk

Individuals in this group are designated by the Associate Director, ITS Operations

Unlocking of AD accounts:
An account gets locked out by a user or a process when more than 5 invalid login attempts have occurred. When this happens, the desired course of action is for the user to call the UNMC ITS Customer Support Services Help Desk at 559-7700 requesting an account unlock. The Help Desk then unlocks the account.

Resetting AD passwords:
If a user forgets their AD password, the desired course of action is to call the UNMC ITS Customer Support Services Help Desk at 559-7700 requesting a password reset. The Help Desk verifies the identity of the user. Upon successful validation of the user's identity, the Help Desk resets the user's password, sends a confirmation email, and sets the flag to force a password change.

In the case where the validation database appears to be in error, students will be referred to Student Services and employees to their PAF coordinator in order to correct the database. The Help Desk will treat this as an emergency situation and work with Help Desk management to determine the next steps.

If the Help Desk is unable to validate a non-employee (contractor, etc), then that individual's business sponsor must call the Help Desk to verify the caller's identity on behalf of her/him. The Help Desk will then verify the business sponsor’s identity and
upon successful validation the password will be reset. If the Help Desk is unable to validate the manager of the non-employee, then Help Desk personnel will work with the Help Desk management to determine the next steps.

**Enabling a Disabled Account**

No password will be reissued if an account is disabled. If an account is disabled, the person who disabled the account should be contacted for the ongoing handling of the issue. If the person who disabled the account is unavailable and it is an emergency, please contact the Help Desk Manager.

No password will be given to anyone other than the user except with the permission of HR or General Counsel or when Emergency Circumstances exist. The Help Desk Manager will review the emergency circumstances and determine the next steps.

4. **Authorities and Administration**

   Assistant Vice Chancellor, Information Technology Services
   Information Security Officer
For this example the fields we have in our database for this person are as follows...
First Name = Elizabeth
Last Name = Smith
Middle Initial = Q
Nickname = Beth

<table>
<thead>
<tr>
<th>Seq No</th>
<th>Criteria</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>nickname.last</td>
<td><a href="mailto:beth.smith@unmc.edu">beth.smith@unmc.edu</a></td>
</tr>
<tr>
<td>2</td>
<td>nicknamemi.last</td>
<td><a href="mailto:bethq.smith@unmc.edu">bethq.smith@unmc.edu</a></td>
</tr>
<tr>
<td>3</td>
<td>firstletterofnickname.last</td>
<td><a href="mailto:bq.smith@unmc.edu">bq.smith@unmc.edu</a></td>
</tr>
<tr>
<td>4</td>
<td>firstletterofnicknamemi.last</td>
<td><a href="mailto:bq.smith@unmc.edu">bq.smith@unmc.edu</a></td>
</tr>
<tr>
<td>5</td>
<td>first.last</td>
<td><a href="mailto:elizabeth.smith@unmc.edu">elizabeth.smith@unmc.edu</a></td>
</tr>
<tr>
<td>6</td>
<td>firstmi.last</td>
<td><a href="mailto:elizabethq.smith@unmc.edu">elizabethq.smith@unmc.edu</a></td>
</tr>
<tr>
<td>7</td>
<td>firstletteroffirst.last</td>
<td><a href="mailto:e.smith@unmc.edu">e.smith@unmc.edu</a></td>
</tr>
<tr>
<td>8</td>
<td>firstletteroffirstmi.last</td>
<td><a href="mailto:eq.smith@unmc.edu">eq.smith@unmc.edu</a></td>
</tr>
<tr>
<td>9</td>
<td>nickname.lastnumber (as a last resort use sequential number starting with 2 until finding one not in use)</td>
<td><a href="mailto:beth.smith2@unmc.edu">beth.smith2@unmc.edu</a></td>
</tr>
<tr>
<td>10</td>
<td>first.lastnumber (as a last resort use sequential number starting with 2 until finding one not in use)</td>
<td><a href="mailto:elizabeth.smith2@unmc.edu">elizabeth.smith2@unmc.edu</a></td>
</tr>
<tr>
<td>GPO</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Default Domain Policy</td>
<td>User Default policy</td>
<td></td>
</tr>
<tr>
<td>CME Tracker</td>
<td>Access to Continuing Ed site</td>
<td></td>
</tr>
<tr>
<td>Outlook</td>
<td>Outlook template settings</td>
<td></td>
</tr>
</tbody>
</table>