1.0 Purpose

This policy defines the general structure of AD in regards to management delegation, and the recommendation(s), qualifications, and rights of delegated OU Administrators (OUAs).

2.0 Scope

The policy shall apply to all Eastern Michigan University staff members who request the authority (or have the authority requested on their behalf) to become an Organizational Unit Administrator (OUA) to manage an OU in AD.

3.0 Policy

**OU Design & Delegation**

OUs will be automatically created by the Active Directory Administrators (ADA) group for each unit (college or division) of the university. Each University entity may have its own OU. OUAs will be delegated access to the appropriate OU(s) based on their job function within the University.

**OUA Recommendation(s)**

Upon approval of the ADA group, an OUA will be granted the authority to manage an OU. Because this authority can significantly affect the computing resources of a unit, staff members must be recommended by the college or divisional head to be delegated as an OUA for a unit. This recommendation must be submitted to the ADA group in writing by the appropriate college or divisional authority. The ADA group will typically review submissions within 10 business days of submission, and will respond in writing. The response will include either approval of the requested OUA, or with specific reason(s) why the request was denied. Any denied requests can be appealed to the Senior Director User Services and / or the Senior Director Enterprise Systems in writing.

**OUA Qualifications**

OUA candidates should be fluent in AD technology per standard 6.4.1S. They should have, at minimum, a conceptual understanding of the major components of AD including forests, domains, OUs, sites, Group Policy Objects (GPOs), and domain local, global, and universal security groups. They should also have an understanding and some basic experience with the standard troubleshooting steps and tools available for handling Group Policy issues, such as the use of the Resultant Set of Policies (RSOP) tool.

Certifications held by the candidate relevant to Active Directory can be used as reasonable indicators that a staff member is appropriately qualified to become an OUA.

Further qualifications for approval of an OUA may be required by the ADA group based on the university function(s) of the requesting unit and its specific AD management requirements. Any necessary qualifications specific to the unit will be reviewed with the requestor upon submission of the OUA delegation request.

**OUA Rights**

OUAs have the ability to create (add), modify, and delete computers, groups, and GPOs in their delegated OU(s). User objects will be added to an OU upon request of the OU’s OUA to the ADA group, and must only consist of the type of users necessary for service accounts.
**DoIT support for OUAs**

DoIT staff in the ADA group provides support to OUAs in local units. OUA support shall be provided in response to e-mails sent to ad-admins@emich.edu. AD Administrators are generally available to handle support requests from OUAs during normal business hours.

The ADA group will be expected to:

- Communicate and coordinate with (OUAs) to minimize disruption to end users.
- Notify OUAs about all scheduled maintenance.
- Work with OUAs to restore deleted AD objects.
- Meet response and resolution times associated with service-related incidents.

For more information, please refer to EMU’s IT Policy web site.

---

**4.0 Responsibility for Implementation**

The Director of Network and Systems shall have the authority and cause this policy to be implemented and maintained.

---

**5.0 Enforcement**

The ADA group reserves the right to revoke OUA privileges when an OUA is found in violation of this policy or its associated procedures, standards, or guidelines. Any revocation can be appealed to the CIO in writing.

Any employee found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under University policy. Any student found to violate federal or State of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under EMU’s Student Code of Conduct. Any suspected violation of state or federal laws will be reported to the appropriate legal authority for investigation.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

---

**6.0 Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory® (AD)</td>
<td>A centralized directory service for networked computers that enables central management of authentication, user accounts, applications, and policy enforcement. Active Directory® is a registered trademark of Microsoft Corporation. All trademarks are property of their respective owners.</td>
</tr>
<tr>
<td>AD Objects</td>
<td>Computers, groups, users, and group policy objects.</td>
</tr>
<tr>
<td>AD Administrators (ADA Group)</td>
<td>DoIT staff members who have responsibility for administering the AD forest, domain, and services, as defined by the Director of Network and Systems.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>A container for holding computers, groups, and applying group policies.</td>
</tr>
<tr>
<td>Organizational Unit Administrators (OUAs)</td>
<td>Local / college technical staff members who have been delegated rights which enable them to manage AD objects for a unit.</td>
</tr>
</tbody>
</table>

---

**7.0 Revision History**

<table>
<thead>
<tr>
<th>Description</th>
<th>Approval Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>References include the University of Minnesota OIT policies regarding AD and the University of Maryland’s Active Directory Policies.</td>
<td>October 19, 2011</td>
</tr>
<tr>
<td>Updated</td>
<td>November 14, 2012</td>
</tr>
</tbody>
</table>