

Attachment E

AD OU Structure Standard

**COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY STANDARD REQUEST**

SUBJECT:	ACTIVE DIRECTORY ORGANIZATIONAL UNIT STRUCTURE STANDARD	ADOPTION DATE:	
REQUESTER:	EXECUTIVE INFORMATION TECHNOLOGY COUNSEL (EITC)		
APPROVER(S):	COUNTY BOARD OF SUPERVISORS		
VERSION:	1.0	PAGE:	PAGE 1 OF 3

I. Standard Overview

This standard defines the Active Directory organizational unit structure and associated naming conventions to be used in the County's Active Directory.

II. Standard Origin

Support Renew '22 initiative RD-4.01. This would implement a policy for standardizing technologies with the intent of reducing training, support costs, improving security, and sharing applications.

III. Scope

The standard applies to all organizational units in the County of Santa Barbara Active Directory as defined in this document.

IV. Definitions

1. Active Directory (AD): a Microsoft technology used to manage users, computers and other devices on a network.
2. Organizational Unit (OU): a container within the Active Directory for creating security boundaries, and organizing the structure of the Active Directory implementation.
3. Daily User Accounts: Active Directory accounts used by employees to login to the County network. External systems will synchronize with this OU to populate user accounts used for identity and authentication.
4. Office 365 Resource Accounts: A disabled user object in Azure AD and can be used to represent resources in general in exchange it may be used to represent conference rooms. These accounts do not require licensing in Office 365.

V. Standard Application

IT Professionals will apply the standard as part of domain structure creation and maintenance tasks.

**COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY STANDARD REQUEST**

SUBJECT:	ACTIVE DIRECTORY ORGANIZATIONAL UNIT STRUCTURE STANDARD	ADOPTION DATE:	
REQUESTER:	EXECUTIVE INFORMATION TECHNOLOGY COUNSEL (EITC)		
APPROVER(S):	COUNTY BOARD OF SUPERVISORS		
VERSION:	1.0	PAGE:	PAGE 2 OF 3

I. Standard

The following OU's are required in the shown hierarchy except as noted:

i) <Departmental OU>

- (a) Admins – This is to contain .ad accounts only. No standard user accounts. Security Groups for Admin accounts are OK as well.
- (b) Computers – This should contain all departmental computers. We can use wmi filtering to apply GPO's to specific Operating Systems, and many other properties.
 - 1. Kiosk – This OPTIONAL OU would contain Computers that have limited user access.
 - 2. NetMotion – This would contain any computer running NetMotion.
 - 3. Disabled – OPTIONAL OU. ²
- (c) Email – Distribution Groups, Contacts, Office 365 Resource Accounts, Conference Rooms, Calendars, Shared Accounts. These will be synchronized to Office 365 or other email related systems.
- (d) Groups – This OU will contain Security Groups, and may have Sub OUs.
 - 1. Printers – This OPTIONAL OU would contain Security Groups for GPO based printer deployment.
- (e) LocalAdmin – This is to contain .la accounts only. No standard user accounts. Security Groups for .la accounts are OK as well.
- (f) Miscellaneous – Objects in this OU will not be synchronized to external systems. It may contain any number of sub OUs to contain service accounts, external user accounts, etc.
- (g) Servers – This OU will contain any departmental server computer objects. Sub OUs as needed to block GPO inheritance.
- (h) Staff¹ – This OU will only contain Daily User Accounts, one account per user. Specifically accounts that would be synched with any other system. Sub OU's are to be used for logical separations and inheritance blocking only. Logical separations would be items such as geographic locations, or programs.²
 - 1. Disabled – OPTIONAL OU. Disabled account may be placed here. ²
- (i) Test – This OU is for emulating your production OU to test GPO settings on a limited number of users. Test Accounts belong here.

¹ See AD Attribute Standards for the use of Employee-Type attribute to distinguish between regular, extra help, contractors.

² Accounts shall be disabled for 24 hours before being deleted to allow attributes to be synchronized to external systems. It is difficult for a system to recognize an object that used to exist is now missing. Giving it 24 hours in a disabled state allows the system time to recognize a change in status.

**COUNTY OF SANTA BARBARA
INFORMATION TECHNOLOGY STANDARD REQUEST**

SUBJECT:	ACTIVE DIRECTORY ORGANIZATIONAL UNIT STRUCTURE STANDARD	ADOPTION DATE:	
REQUESTER:	EXECUTIVE INFORMATION TECHNOLOGY COUNSEL (EITC)		
APPROVER(S):	COUNTY BOARD OF SUPERVISORS		
VERSION:	1.0	PAGE:	PAGE 3 OF 3

II. Related Standards:

Active Directory Data Standards

III. Referenced Documents:

End User Computing Standard Business Case