ACTIVE DIRECTORY MANAGEMENT

Goal: In order to serve our user community in an effective and efficient manner, the Information Technology Departments of the Contra Costa Community College District agree to cooperate in the management of Active Directory in the following ways:

Definition: Active Directory services are repositories for information about network-based entities such as applications, files, printers, and people. Directory services are important because they provide a consistent way to name, describe, locate, access, manage, and secure information about these resources. Active Directory allows organizations to manage and share information on network resources and users within a structure otherwise known in Microsoft terms as a forest.

Procedure: This is a living document and will be reviewed and modified as necessary, but at least yearly.

1. Active Directory Structure

A single administrative forest active directory is implemented. A separate student forest will be determined by each college. This single forest will include a domain for each major location as well as an empty root domain to house the enterprise and schema administrator privileges. Costs associated with maintenance, warranty, and upgrade of the empty root domain will be the responsibility of the District Office. The domains will be peers of each other. Each technology group is solely responsible for the administration of their domain. Costs associated with maintenance, warranty, and upgrade of each site's domain will be the responsibility of the site. This forest encompasses only administrative users and resources.

The empty forest root domain will have a DNS (Domain Name Service) domain of collegesofcc.cc.ca.us and a Netbios name of CCCCD. There will be two domain controllers named Kraken and Leviathan.

Each site will retain its own DNS name space.

2. Active Directory Security

The security of the empty forest root domain is the most important security concern of active directory. Best practices for domain controllers, enterprise administration and domain administration accounts are included in this cooperative agreement. In addition, two-factor authentication will be utilized exclusively in the empty forest root domain. This authentication requires a valid user name and password as well as a physical token.

The empty forest root domain will be monitored 24x7 utilizing Microsoft Operations Manager for successful or failed login attempts. Any successful login attempt will be checked by District Information Technology against completed change management requests. Event logs will be backed up on another server to ensure they are not tampered with in the event of a breach and will be provided to enterprise administrators upon request. The enterprise administrator group is comprised of the college technology deans, technology supervisors, and the District Office technology management staff.

In the event of a suspected breach, District Office enterprise administrators will disable all enterprise administration accounts immediately until passwords can be changed. If a College administrator suspects a breach, the District Office should be notified immediately. An incident response form will be completed

(over)

and provided to enterprise administrators. Additionally, each site will be notified by telephone utilizing a phone tree in an attempt to make a live connection. Any security concern within the forest is a top priority and will be given the full attention of the necessary technology staff. The enterprise administrator group will monitor, review, and discuss breaches and take appropriate action.

3. Standardized Best Practices for Security of Domain Controllers (DCs)

The DCs house the entire database of their domain as well as limited data about the structure of the forest. As such, these servers must be strongly safeguarded both electronically and physically as follows:

- All administrative DCs will be secured at all times in a room or closet accessible only by authorized information technology staff.
- DCs will be installed with antivirus software and configured for daily updates.
- DCs will only be configured with NTFS partitions.
- Backups of DCs will be physically secured and destroyed when obsolete.
- DCs will be behind firewalls.
- DHCP should not be run on DCs.
- Web services should not be run on DCs.

4. Change Management for Forest-Wide Changes

Forest-wide changes require the use of enterprise administrator privileges such as:

- Addition or deletion of a domain
- Installation of software that will modify the schema
  - Project leaders are responsible for identifying possible schema impacts as part of their planning and including that information as part of the change management process
- Requests to modify the schema
- Authorizing new DHCP servers
- Change of IP on DNS name servers that are referenced by stub zones in the forest.

A change management form for an impending change will be completed as early in advance of the desired implementation date as possible, with a targeted goal of two weeks. The purpose of this process is to prevent system conflicts among sites by notifying others of upcoming changes, to ensure that there are no negative consequences as a result of the modification, and to provide other sites ample time to explore potential system conflicts. The technology managers group at each site will signify there are no system conflicts by approving the change management form.

The Enterprise Administration Group will have individual login rights to make necessary forest-wide changes. The DO network staff will have backup operator rights in order to perform nightly backups of the root domain. Microsoft Operations Manager will be used to monitor the overall health of active directory, watch for security events, and remotely backup the event logs.

5. Enterprise Administration Group

Due to the significant privilege level of these accounts, they should not be used unless needed for a project that has completed the change management process. In the event of an emergency and when time is of the essence, verbal notification will be provided to at least one enterprise administrator at each site. The change management form will also be completed for change management tracking purposes. To help ensure the security of these accounts, full auditing of account usage will be maintained and these accounts will conform to the following security best practices:

- Each member of the Enterprise Administration Group will have only one Enterprise Administration account which will reside in the forest root domain.

- The account will be developed as follows: LastNameFirstName. No other windows logon will use this login schema.
- Account name must be different than any other windows logon.
- Password must be complex, consisting of uppercase, lowercase, numbers and non-alpha.
- Passwords must be at least 15 characters in length. This prevents AD from creating backwards compatible hashes which are less secure.
- Passwords will only be provided in person or verbally. They must never be sent electronically.
- If passwords are stored electronically, they must be secured using an accepted industry encryption.
- Two-factor encrypted authentication is required for all enterprise administration accounts.

6. Domain Administration Groups

It is recommended that each group adopt as many of the enterprise administration best practices as possible. At the least, a technician's domain administration rights should belong to a separate account than their personal user account. This minimizes the exposure of their privileged account. Auditing of the domain administration groups and accounts should occur on a regular basis to ensure that no additional accounts or rights have been granted without due consideration. AD offers much more granular rights management and where possible, people should be granted only those rights they must have.

7. Exchange Administration

a. Roles

Operating system and exchange software administration will reside with District Office staff. Each site will select up to three domain administrators to perform the college exchange related tasks. The three administrators will be granted Exchange review access and account operator rights in the 4cd-domain. These permissions allow the following:

- View the mail queues on the exchange server
- View mailbox size
- View public folders and their properties
- Create a new mailbox for a user at user account creation
- Delete a user (this does not automatically delete the mailbox)
- Add members to a list
- Remove members from a list
- Change the mailbox size of individual users
- Change email addresses of individual users
- Add or delete lists*

*List administration tasks will be shared between the college and the District Office IT groups. The District Office IT group is responsible for creation, deletion, and changes to properties of lists. Both groups will manage the list memberships as they change.

The District Office IT group will have account operator permissions in each domain to support troubleshooting of any potential user issues.

b. Standards

The firewall(s) at each site must be configured to allow Exchange servers and domain controllers to communicate with one another.

(over)

Each site administrates the DNS for its domain. Since DNS houses the records for the Exchange server, the DNS records for the servers may not be modified or moved unless previously agreed to via change management.

User accounts in all domains will be displayed by *LastName, FirstName* (e.g. Seaberry, Ben). User login will maintain existing 8 character maximum format of *FirstInitialLastName* (e.g. BSeaberr).

Email addresses consist of *FirstInitialLastName* (e.g. BSeaberry). In the event of a conflict, the standard will be *FirstInitialMiddleInitialLastName* (e.g. BXSeaberry). If a non-standard email address is created, pertinent information will be logged by the mailbox creator using a form on the intranet at *http://gryphon.4cd.net/webapps/emailform*.

Distribution lists will reside in the 4cd-domain and will utilize existing naming standards (e.g. 00 for districtwide, 01 for DO, 02 for DVC, etc).

Exhibit A outlines the consistent manner in which user accounts must be created.

8. Notification Process

If forest-wide issues are encountered, the District Office will notify each site technology manager who will in turn determine and communicate the necessary course of action for their site. If a site manager cannot be reached, a District Office manager will take appropriate action.

If domain-level issues are encountered, the site will determine the appropriate course of action.

9. Approvals

Approval Date: September 14, 2004

Phyllis Gilliland
Acting Chancellor - District Office

Mark Edelstein
President - DVC

Helen Carr
President - CCC

Peter Garcia
President - LMC

Tom Smith
Vice Chancellor, Finance and
Administration - District Office

Mojdeh Mehdizadeh
Vice Chancellor, Technology Systems Planning
and Support - District Office

Jeffrey Kingston
Vice Chancellor, Facilities and
Operations - District Office

Historical Annotation:
Adopted 9/14/04

Office of Responsibility:
Technology Systems Planning and Support

Exhibit A
Correlation of AD Users and Computers Fields to Outlook Properties

Below is a description of the data to be entered into the common fields as well as the formats. Following the common fields are descriptions of some of the tabs not mentioned previously.

1. **First name -** Under the general tab in both programs. First initial should be capitalized.
2. **Initials -** Under the general tab in both programs. Users that must use the middle initial in their login due to duplicate accounts in the domain must have this field completed. Middle initial should be capitalized.
3. **Last name -** Under the general tab in both programs. First initial should be capitalized.
4. **Display name -** Under the general tab in both programs. This field is used to display the user in the Global Address List and should be Lastname, Firstname MiddleInitial with the first initials capitalized. (Seaberry, Ben)
5. **Alias –** Under the general tab in Outlook and the exchange general tab in ADUC. The alias is used to initially create the email address.
6. **Address -** Under the general tab in Outlook and the address tab in ADUC. This should be completed with the address for the user's location. Be sure to spell out all abbreviations (e.g. Road rather than Rd.).
7. **City -** Under the general tab in Outlook and the address tab in ADUC. This should be completed with the city for the user's location.
8. **State -** Under the general tab in Outlook and the address tab in ADUC. This should be completed with the state for the user's location.
9. **Zip Code -** Under the general tab in Outlook and the address tab in ADUC. This should be completed with the zip code for the user's location.
10. **Country/Region –** Under the general tab in Outlook and the address tab in ADUC. Enter USA.
11. **Title -** Under the general tab in Outlook and on the organization tab in ADUC. This field is not the description field found on the general tab of ADUC. This should be the job title for the user. For full time faculty it should be "Faculty". Part time faculty should be coded "Faculty (Part-time)". All managers and classified should have their official job title listed. All hourly classified should be coded as "Hourly" followed by the job title (e.g. Hourly Office Assistant I).
12. **Company -** Under the general tab in Outlook and on the organization tab in ADUC. This should contain the name of the user's location and be fully spelled out (e.g. Diablo Valley College).
13. **Department –** Under the general tab in Outlook and on the organization tab in ADUC. In the case of faculty, this should contain only the department the user is a member of, not divisions. Consistent, fully spelled out descriptions should be used (e.g. Mathematics, NOT Math).
14. **Office** - Under the general tab in both programs. It should include the room or floor where the user works.
15. **Assistant** - Not populated.
16. **Phone** - Under the general tab in both programs. This should include the full phone number of the location and the user's extension. (e.g. (925) 229-1000 x1295).
17. **Manager** - Displayed on the organization tab in both programs. When populated for an employee, they will be displayed as a direct report for the person listed as Manager. To specify the manager, click on the change button and select the person from the address list. (Optional)
18. **Direct Reports** - Displayed on the organization tab in both programs. It is only populated for managers that have been added to the manager field of their employees. (Optional)
19. **Business** - Under the Phone/Notes tab in Outlook and the General tab with field labeled telephone in ADUC. It should be the same as the phone field on the general tab.
20. **Home** - Under the Phone/Notes tab in Outlook and the Telephones tab in ADUC. This field will be empty. (Optional)

(over)

21. **Mobile** - Under the Phone/Notes tab in Outlook and the Telephones tab in ADUC. This field will be empty. (Optional)
22. **Fax** - Under the Phone/Notes tab in Outlook and the Telephones tab in ADUC. This field should include the fax number the user would list on their business card.
23. **Pager** - Under the Phone/Notes tab in Outlook and the Telephones tab in ADUC. This field will be empty. (Optional)
24. **Notes** - Under the Phone/Notes tab in Outlook and the Telephones tab in ADUC. This may contain any notes on the user. For temporary or generic accounts it will contain the person responsible for the account. For non-standard email addresses, enter "non-standard" in addition to the reason for creating the non-standard address (e.g. non-standard due to duplicate name).
25. **Group membership** - Under the Member tabs of both programs, however it displays different data depending on the program. In Outlook it displays the email distribution groups that the user is a member of. In ADUC it displays the security groups and distribution lists that the user belongs to. These will not match, but ADUC will contain the distribution lists and this is where you will add the user to distribution lists.
26. **Email Addresses** - These are tabs in both programs. This lists the email addresses associated with user. The standards for the email addresses by site are detailed later in this document. In ADUC the Primary SMTP address is bold. This address is what will be used to send emails and for the reply-to address.

Screen prints

Screen prints of all the tabs in an AD Users and Computers (ADUC) profile for a single user and screen prints of all the tabs in the Outlook properties for the same user can be found at:

http://gryphon.4cd.net/technology/network/Forms/AllItems.aspx

Tabs in ADUC that are not displayed in Outlook but may need to be used:

Exchange General – This tab has the Alias field but also contains the button for Storage Limits. It opens a page where the storage limits for the user's mailbox are set. The limits by site will be defined later in this document. Most users should have the Use mailbox store defaults set. Changes to a user's mailbox size must be approved by the appropriate technology manager/dean.

To give someone a higher limit, uncheck the Use mailbox store defaults checkbox, then check the three checkboxes and enter a KB value for the size needed. All users, regardless of mailbox size, have the Use mailbox store defaults checkbox set for Deleted item retention.

Email address formats by site:

All users at all sites will have an X.400 email address. These should not be modified or removed.

- DO – FirstInitialLastName@4cd.net
- CCC – FirstInitalLastName@contracosta.edu
- DVC – FirstInitalLastName@dvc.edu and FirstInitialLastName@diamond.dvc.edu . The dvc.edu address must be the primary.
- LMC – FirstInitialLastName@losmedanos.edu. Other addresses may automatically be spawned but should be deleted.
- SRVC – FirstInitalLastName@srvc.net

Mailbox size limits by site:

DO – 30 mb
CCC – 15 mb
DVC – Based on user
LMC – 30 mb
SRVC – 15 mb