ACCOUNT MANAGEMENT AND ACCESS CONTROL
STANDARDS AND PROCESSES
July 12, 2007

Updated August 3, 2007 – Company field definitions enhanced and Volunteer value added; ACF2 naming exceptions documented.

Introduction

In order to maintain the integrity and security of the County's computing infrastructure and automated systems, the County has established standards and procedures for Access Control [specifically for Active Directory (AD) and Mainframe Security (ACF2)] to ensure only authorized or verified users have access to the County's Network and Mainframe.

Responsibilities

- OHR creates and is responsible for Employee IDs and records in HRMS and UDM
- DTS manages the AD and ACF2 systems
- Departments may designate Administrators for AD and ACF2 and ensure by providing acknowledging documentation that they attend any requisite training, as defined by DTS.
- Department Administrators create and are responsible for maintaining Accounts in AD and ACF2
- Department Administrators are responsible for ensuring that Accounts are deactivated promptly when person identified in the account no longer requires or is authorized to have access.
- Administrators that do not perform updates are not required to attend training, but must validate accounts and provide DTS information requested for updates.
- Administrators perform a periodic review of all accounts either created or approved by local departments for valid and authorized accounts.

AD Naming Convention and Standard Requirements

When Department Administrators create accounts, they must follow established naming and other standard requirements as detailed below.

The AD **Userid** must be unique and have 6 characters followed by the lowest available 2 digit integer

1. For most user accounts the ID will be the first 5 letters of last name plus the first initial of the first name plus a two digit integer. Example, Ann Johnson = johnsa01.
2. For users with short last names use additional letters of the first name to meet the six character requirement. Example, John Doe = doejoh01.
3. For users with short first and last names use x(s) to meet six character requirement. Example, Mao Li = limaox01.
4. If the ID already exists, increment the integer portion of the ID until it is unique. Example, Ann Johnson = johnsa02
5. Resources and public/shared mailboxes also need to be 8 characters and follow the naming conventions as documented in AD administration training materials. Shared ID's must be reviewed on a monthly basis to ensure that all users are identified.

The **Department** field must be the same as the OU (Organizational Unit)

The **Company** field must be one of the following

- **MCG** – Montgomery County Employee, paid interns
- **Retired** – Retired , Terminated, and Deceased Employees

- **Contractor** – An account used by someone under contract to the County
- **Partner** – An account used by a County business partner, examples: municipalities, health provider, commission members, etc.
- **System** – An account used by a system administrator
- **Training** – An account used for training purposes
- **Volunteers** – Volunteers, unpaid interns
- **Resource** – Shared mailbox, resource mailbox, and any account not described above

In addition, the following fields must not be blank for MCG, Retired, Contractor, Partner accounts: First Name, Last Name, Office, Address, and Telephone number. N/A should be used when a field is not applicable or data is not available.

AD Account Compliance Processes

On-going: DTS will deactivate AD accounts that do not meet the standards detailed above, as they are discovered. No notifications will be sent. Account corrections must be submitted, in writing to DTS, prior to reactivation.

Daily: Automated systems managed by DTS and OHR will reconcile all employee accounts AD with HRMS. The system will notify Department Administrators via email if any unmatched records exist in their department and the Administrator will manually reconcile all un-reconciled records by updating the AD account or manually matching the account with an HRMS record in UDM within 10 business days.

Monthly: DTS will deactivate all accounts of employees that HRMS reports were terminated during the prior month (if not already deactivated by the Department).

Automated systems managed by DTS will send reports to Department Administrators listing all accounts that have not been used in past 90 days. Department Administrators will review, deactivate, delete accounts, or assist users in changing their password, as appropriate within 10 business days. At the end of the 10 business days, DTS will deactivate any remaining accounts that have not been accessed/updated. Accounts that were disabled the previous month will be processed as any account no longer in use – all groups stripped, mailbox deleted, and moved to the "Inactive" folder. The account will remain disabled.

Every 3 Months: Automated systems managed by DTS will send reports to Department Administrators listing all non-employee accounts. Department Administrators will review, update, deactivate, or delete accounts as appropriate and send confirmation thereof to DTS within 10 business days.

ACF2 Naming Convention and Standard Requirements

When Department Administrators create accounts, they must follow established naming and other standard requirements as detailed below. (Note: DTS acts as the administrator for several departments)

The ACF2 **Userid** must be unique and have 7 characters

1. The first 3 characters will be from the list of approved department/group identifiers
2. The 4th and 5th characters will be lowest unique integer starting with 00
3. The 6th and 7th character will be the person's initials

Exceptions: Corrections is COR followed by a three digit number, Sheriff is SHR followed by three numbers and Montgomery County Police is MCP followed by three numbers. Staff in these departments may have a state assigned id which is a single Alphabetic character followed by a 5 digit number.

ACF2 userids requiring ADPICS and/or FAMIS access will be assigned by DTS or Finance.

The **Company** field must be one of the following

- **MCG** – Montgomery County Employee
- **RET** – Retired Montgomery County Employee
- **CON** – An account used by someone under contract to the County
- **PAR** – An account used by a County business partner, examples: municipalities, health provider, commission members, etc.
- **SYS** – An account used by a system administrator
- **TRA** – An account used for training purposes
- **OTH** – Any account not described above

- **MCG** – Montgomery County Employee, paid interns
- **RET** – Retired , Terminated, and Deceased Employees
- **CON** – An account used by someone under contract to the County
- **PAR** – An account used by a County business partner, examples: municipalities, health provider, commission members, etc.
- **SYS** – An account used by a system administrator
- **TRA** – An account used for training purposes
- **VOL** – Volunteers, unpaid interns
- **RSC** – Shared mailbox, resource mailbox, and any account not described above

If the user also has an AD account, then the **Telephone** field must contain the AD userid, otherwise the field must contain a valid phone number for the user or person responsible for the account.

The **Name** field must not be blank and must be ordered by: Last Name, First Name.

ACF2 Account Compliance Processes

On-going: DTS will deactivate ACF2 accounts as they are discovered that do not meet the standards detailed above. No notifications will be sent. Account corrections must be submitted, in writing to DTS, prior to reactivation.

Monthly: DTS will deactivate all accounts of employees that HRMS reports were terminated in the prior month.

Every 3 Months: DTS will deactivate all accounts that have not been used in past 90 days.
DTS will send reports to Department Administrators listing all non-employee accounts. Department Administrators will review, update, deactivate, or delete accounts as appropriate and send confirmation thereof to DTS within 10 business days.