



## Generic Account Policy

**Approved:** September 6, 2008  
**Effective:** September 10, 2008  
**Policy:** 95-01-01-04

**Amended:**  
**Expires:**

### I. PURPOSE

To establish the policy for the process of Creating and Maintaining Generic Core Accounts for Network and System access.

### II. ACCOUNTABILITY

The Vice President of Information Services and Technology (IST), IST Director(s) and school / unit IT Management shall ensure compliance with this policy.

### III. APPLICABILITY

This policy applies to all School and Unit Technology groups responsible for account maintenance associated with the University Active Directory structure. It includes all Generic accounts under the UMDNJ.EDU Active Directory umbrella, specifically known as and referred to as "Core Accounts".

### IV. DEFINITIONS

- A. Generic Account – is considered an account that is not derived using the Faculty, Staff or Student naming convention. There is no corresponding RUID associated with a generic account. This account name is derived using the device naming convention and applying this to a user object.
- B. RUID – Reserved User ID, also known as an employee account. This account is derived using the Faculty, Staff and Student naming convention. The RUID is comprised of the individuals surname, first name and middle initial.
- C. RUID Account – accounts that are derived utilizing the University RUID naming convention and assigned to Faculty, Staff and Students.
- D. Audit – the process of validation that, the policy as written, is being met with regard to specific details.

### V. REFERENCE(S)

- A. Naming Convention Standard document (**CURRENTLY UNDER REVISION**)

## VI. POLICY

### A. General Principles:

All generic user accounts must be given the same attention as RUID accounts and be de-provisioned when no longer needed. These accounts must be validated by the requestor associated with the account at the time of audit. If the audit results in it no longer being needed the account will be deleted by CST.

### B. Requirements:

1. To ensure that only necessary accounts have access to the network and Active Directory structure.

All Generic accounts will be validated twice a year, June and December. CST will run an account query validating the frequency of Generic account use. Accounts that have not logged into the network in the last 45 days will be validated for need and deleted if no longer in use.

### C. Responsibilities:

#### 1. CST Directory Administrator:

- i. Prepare a spreadsheet of “flagged” Generic accounts that have not accessed the network in 45 days. The spreadsheet must contain the individual requestor of the account.
- ii. Correlate the Generic account information for distribution to IT Technology groups.
- iii. Delete required accounts based on Technology group validation results.

#### 2. IT Technology Group:

- i. Validate the need of the flagged accounts and report the results to the CST Directory Administrator for action.

## VIII. PROCEDURE(S)

A. CST will distribute the required spreadsheet to the IT Technology groups via email. The timeframe for the audit will be communicated through the CST partner meeting, including the completed response information, prior to distribution.

B. The IT Technology Group will update the spreadsheet validating the need by placing a Y/N in the account required column.

C. All acknowledged deletions will be completed by the CST Directory Administrator and completed spreadsheets will be kept on file with CST.