Network Account Retention and Terminations Policy
Des Moines Area Community College

July 19, 2019

Purpose of Policy

The purpose of this policy is to ensure the proper access, usage and disclosure of Des Moines Area Community College's Active Directory (AD) Solution by its students, faculty and staff. Active Directory Accounts are network user names and passwords allowing access to DMACC resources, including email. These are resources provided by the college to complement traditional methods of communications to support teaching and learning, research, services and administration. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Violations of the policy may result in disciplinary action.

DMACC Services Accessed via Active Directory (AD) Accounts

- Computer Workstations
- myDMACC
- Email Account
- DMACC MyLab
- Online Course Access
    - Blackboard
- Personal File Storage
    - P:\homedrive
    - OneDrive for Business
- Shared File Storage
    - Any shared course or department files
    - OneDrive shared documents
- DMACC Forms
- DMACC Libraries Online Resources

Student AD Access and Retention Policy

Student Active Directory Accounts remain active as long as the student maintains credit enrollment at Des Moines Area Community College.

- Student AD Accounts
    - Student information will be kept 9 months from the end of the last semester attended. If the student is not registered for any classes after the 9-month period and the student is not an employee, all information will then be removed.
- Granting Access to AD Accounts
    - Faculty/Staff needing access to a student's personal Active Directory information (files, email, etc.) will need to contact the VP, Enrollment Services & Student Success.
- Returning Students
    - Students registering for classes after being removed will be re-created in AD as a new user account.

Faculty / Staff AD Access and Retention Policy

Active Directory Accounts will be maintained until notification is received from Human Resources or the department that an individual is no longer employed by Des Moines Area Community College.

- Regular Faculty / Staff Separations other than Terminations for Cause
  - Tech Support should be notified before the separation date to ensure the AD account is disabled at final day's end.
  - AD File Storage
    - Data will remain available for 30 days following the separation date. All information will be removed after the 30 days.
    - During this 30-day period, and with Human Resources approval, a supervisor may contact Tech Support requesting copies of former employees' personal files.
  - AD Email Account
    - Access is available for 30 days following separation date. All information will be removed after 30 days.
    - Email Forwarding: With Human Resources approval a supervisor may contact Tech Support requesting the former employee's email be forwarded to their account for business purposes.
- Emeritus Approved Employees

  Human Resources Procedures Number: HR 3812
  - Eligible faculty and senior administrative/professional employees Active Directory accounts will be maintained following their retirement from the college. The college reserves the right to revoke the title in the event the best interests of the college are not being served.
  - Emeritus titles
    - Emeritus Faculty
    - Emeritus Administrator
- Faculty / Staff Suspensions or Terminations Cause
  - Tech Support should be notified when an employee is suspended on or before the separation date to ensure the AD account is disabled.
  - AD File Storage
    - Disposition of files utilized by the suspended or terminated employee is determined on a case by case basis.
  - AD Email Account
    - Disposition of email sent to / received by a suspended or terminated employee is determined on a case by case basis.

Security Policy (Web Info System)

As of August 14, 2006, DMACC has implemented a new security policy for all DMACC users of the Web Info System. The Family Educational Rights and Privacy Act (FERPA) requires institutions to take precautions to protect students' educational records. Because the Web Info System contains confidential educational records, personal information, and employee records, DMACC is concerned about the confidentiality of your information and is taking steps enhance our security processes.

Recommended PIN Standards

PIN's should be:

1. Only known by user.
2. Exactly 6 characters long.
3. A combination of letters and numbers.
4. Changed regularly.
5. Unique from different accounts.

PIN's should not be:

1. Your username or other commonly known identifier (birthdate, student ID)
2. Words found in a dictionary.
3. Any part of your name.
4. Your address or street name.

It is important that you take precautions to protect the confidentiality of your PIN. Never share it with anyone or post it in any manner. If you know or believe someone else knows your PIN, change it immediately. If you believe your account has been compromised, you should report it immediately to DMACC Tech Support.