



Policy: Digital Identity Policy

Effective Date: 1/20/2023

Division: Administration and Finance

I. SCOPE

This policy applies to McDaniel faculty, staff, and students who use McDaniel's technology resources.

II. PURPOSE OF THE POLICY

The purpose of this policy is to:

1. Establish that a single digital identity is created and used for each person that uses McDaniel technology resources.
2. Establish a standard procedure for the structure, creation, and implementation of digital identities and email addresses.

III. DEFINITIONS

1. **Digital Identity:** the username that uniquely identifies each person in any McDaniel campus computing system, server, or resource.
2. **Faculty and Staff Usernames**

Information Technology uses the following standard structure for faculty and staff usernames:

- The first character of the first name (or display name, if provided) in the Colleague Human Resources Information System plus
- The last name in the Colleague Human Resources Information System

If the username is not unique, the following strategy is used for the username:

- The first character of the first name plus
- The middle initial plus
- The last name

If not unique, iterate through the remaining characters of the first name as the second letter of the username.

If not unique, iterate through the remaining characters of the middle name as the second letter of the username.

3. Student Usernames

Information Technology uses the following standard structure for student usernames:

- The first character of the first name (or display name, if provided) in the Colleague Student Information System plus
- The first character of the middle name in the Colleague Student Information System plus
- The first character of the last name in the Colleague Student Information System plus
- 0100

If not unique, increment the sequence number (e.g., 0101) until a unique username is found

4. Display name: Chosen or preferred name.

5. Email addresses

Information Technology uses the following standard structure for email addresses:

- Username plus
- @mcdaniel.edu

IV. PROCEDURES

Digital identities will be created and implemented in the following manner:

1. All McDaniel College digital identities are stored in the college's Microsoft Active Directory system.
2. All McDaniel College accounts require Multi-Factor Authentication (MFA), also known as 2-Step Authentication. MFA is used to ensure that digital users are who they say they are by requiring that they provide at least two pieces of evidence to prove their identity. MFA requires something the user knows (their password) and something they have (a mobile device or phone). When a person accesses a McDaniel Office 365 service from a new device or web browser, the user will enter their password as usual, but they will also be prompted to approve the login with an app or a code that must be entered before they can access the service. Users are required to use one of the following verification methods:
 - Microsoft Authenticator app notification asking the person to complete verification by selecting Approve from the mobile app push notification
 - A verification code from the Microsoft Authenticator app
 - A text message (SMS) is sent to the person's mobile phone with a 6-digit code
 - A call is placed to the person's mobile phone asking to verify the person signing in
3. The college ensures that all computer accounts in campus computing systems have a corresponding entry in the college's Active Directory system.

Policy Contact: If you have questions regarding this policy, please contact the chief information officer.

History of Review/Revisions: 1/20/2023