Policy #:	ITP-32-1	Effective:		Page #:	
Subject:	Password Policy		Audience:	Employees and Students	

1.0 PURPOSE

The purpose of this policy is to prevent the unauthorized use of college-owned networks, servers, computers and equipment, by establishing standards for strong passwords and the protection of user and system passwords.

2.0 SCOPE

This policy applies to all Meredith Community Members using the organization's technology resources, and/or using any device that has access to the technology resources.

3.0 POLICY

All college-owned technology systems; including Email, Web Advisor, and Blackboard must be protected using a user ID and password combination. Passwords are used for user accounts, servers, email accounts, Blackboard, Web Advisor, and web applications. Users of any college-owned system that requires a password must follow the guidelines below for creating passwords (exception - Student Email which is managed by Google):

A. Passwords and account lockout settings for Meredith Community members should be set to the following order to reflect best practices for security:
    i. Minimum password strength: minimum of 9 characters in length and three character classes are required. Character classes are as follows:
        1. Lowercase (a-z)
        2. Uppercase (A-Z)
        3. Numeric digits (0-9)
        4. Symbols (all other printable characters, not including blank space) !@#$%^&*()_+,-|:"<>?,./='~

B. It is important to protect secrecy of password. The following guidelines must be followed when handling passwords:
    i. All user account passwords must be changed every 180 days or the users will be locked out of their account.
    ii. The use of the previous 5 passwords are prohibited.
    iii. User who enter the wrong password after 5 attempts will be shown "invalid login," and will be locked out of their account for 15 minutes.
    iv. 30 minutes will be allowed to reset account after lockout once there has been 5 failed login attempts.
    v. There is a 24 hour password age limit to prevent cycling through old passwords. (**Defined:** you must use your new password for a minimum of 24 hours.)
    vi. Password complexity: enabled.
    vii. Passwords can never be included in unencrypted emails or other forms of electronic communication. Technology Services will never ask for your password via email, and will never send your password via email.
    viii. Never reveal your password to anyone over the phone, including help desk personnel.
    ix. Do not share your password with assistants, coworkers, family members, or friends.
    x. All passwords must be treated as College Confidential material.
    xi. Do not save password on any unencrypted device.

C. Password reminders will be sent to the users in the following intervals:
   i. 15 days
   ii. 10 days
   iii. 4 days
   iv. 2 days
   v. Password expiration notice

D. Any exceptions to this policy must be approved in advance by Meredith College Technology Services.

4.0 REVISION HISTORY

Date	Revision #	Description of Change
4/22/2013	1.0	Initial Creation
2/22/2016	1.1	Update to 3.0 Policy

5.0 INQUIRIES

Direct inquiries about this policy to:

Jeff Howlett, CIO
Meredith College
3800 Hillsborough Street
Raleigh, NC 27607

Voice: 919-760-8828
Fax: 919-760-2325
E-mail: howlettj@meredith.edu