Benedictine University

Information Technology

Password Policy

Last Updated: 07/2022

1. PURPOSE

The purpose of the Benedictine University Password Policy is to help defend against unauthorized access of university systems and services that could result in a compromise of personal or institutional data or negatively impact the mission of the university.

Passwords are an important aspect of information security. They are the front line of protection for user accounts and, subsequently, access to sensitive data. A poorly chosen password, or a password shared with another person, may result in the compromising of network resources and sensitive information. As such, all users, including full- and part-time faculty and staff, are responsible for taking the appropriate precautions outlined in this policy to select and secure their passwords. The purpose of this policy is to establish rules for the creation of passwords, the protection of those passwords, and the frequency of change.

2. AUDIENCE

The scope of this policy includes all personnel who access any Benedictine University information system or are responsible for any computer account (or any form of access that supports or requires a password) on any Benedictine University hosted or contracted (e.g., cloud computing) system.

3. Policy

A. Password Characteristics

1. Passwords must be at least **ten** characters in length.
2. Passwords must contain at least three of the following four characteristics: one upper case letter, one lower case letter, one digit, and one special character, e.g., !, @,(, $.

B. Changing Passwords

1. When receiving a new account, the user is given a temporary password. All temporary passwords are to be changed upon the initial login after receiving a computer account.
2. After the initial login, passwords must be changed at least once every year.
3. In order to curtail attempts to gain illicit access to an account, an account will be locked after five unsuccessful logon attempts.
4. The previous six passwords may not be used when setting a new password.
5. All vendor supplied default passwords must be changed prior to any application or program's implementation to a production environment.

C. Password Protection

1. Passwords may not be inserted into email messages or other forms of clear text electronic communication.
2. Passwords should not be shared with others. If a password is shared with IT support personnel for troubleshooting, then the password must be changed as soon as possible.
3. Passwords may never be written down or stored off-line in an unsecured manner or on-line in clear text.
4. Passwords are not to be revealed over the phone to ANYONE, including technical support personnel. Support personnel must never initiate a call requesting a password.
5. Other password protection hints include:
    - do not include words like “Benedictine,” “password,” or phrases like “Fall2019” in your password. These are easily guessed.
    - do not talk about a password in front of others,
    - do not hint at the format of a password (ex. "my pet’s name"),
    - do not share a password with family members, and
    - do not reveal a password to co-workers while on vacation.

D. Compromised Passwords

If a password holder believes an account or password has been compromised, she or he must report the incident to the appropriate system administrators and/or the Help Desk (630-829-6684 or helpdesk@ben.edu). Accounts determined through automated or other processes found to be compromised will be immediately suspended and reactivation will only occur after the investigation into how the account was compromised is completed.

F. Password Resets

Password resets may only be performed through the self-service reset tool by the user or by authorized personnel (e.g. Help Desk personnel, System Administrators, etc.). To avoid fraudulent requests for password resets, certain verification steps will be taken by the Help Desk. Help Desk personnel may determine the identity of user through personal knowledge of the individual, including visual recognition, voice recognition, etc.

4. Domain and System Administrators

Due to the higher level of access to systems and services, Domain and System Administrators must adhere to stricter password management standards. Specifically:

1. The minimum length of passwords for Domain and System Administrators is twelve characters.
2. When provided by the system, Domain and System Administrators passwords must contain all four complexity characters (i.e., Upper case, Lower Case, Digit, and Special Character).
3. Domain and System Administrators must reset their password at a minimum of every 90 days.
4. Domain administrators must use a separate account when logging into systems as a domain administrator.

4. VIOLATIONS

Any personnel found to have violated this policy may be subject to disciplinary action and loss of access to Benedictine University resources as described in the Benedictine University Acceptable Use Policy.