BURRELL COLLEGE OF OSTEOPATHIC MEDICINE

STANDARD OPERATING PROCEDURES

Passwords	**SOP #: IT.008.01**
Effective Date	5.20.2024
Last Revision/Review	2.1.2026

1. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords and the protection of those passwords.

2. Related Policy/Authority

B2050 – Data Security Policy

3. Faculty/Staff Responsibilities

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on a system that resides at any Burrell facility, has access to Burrell College's networks or stores any non-public Burrell College information. The Chief Information Officer is ultimately responsible for maintaining, updating and implementing this plan.

4. Definitions

Domain Administrator: Users within the domain who have domain-wide access and administrative rights to the domain. Domain Administrator permissions in the domain can set policies and restrictions that apply to all users on the network.

Domain User: Anyone who has a user account and has authenticated within the domain. Their level of rights in the domain depends on the level of access granted to them.

5. Procedural Steps

1. Strong passwords must be used to secure access to critical systems and data. A single compromised password can lead to a significant data breach. Burrell College relies upon you to protect your passwords at all times.
2. Everyone using the College's IT resources must create and use passwords that comply with the College's Password Standard.
3. Your Burrell College passwords are never to be shared with another individual, including Help Desk staff and administrative assistants.
4. Never use your Burrell College password on a non-Burrell College system (e.g. for personal email, banking, or social media site).
5. Avoid writing your passwords on paper (e.g. sticky / post-it notes).
6. All domain user-level passwords must conform to the guidelines described below.
7. All domain administrator-level passwords must conform to the guidelines described below.

GUIDELINES:

1. Domain Administrator
   a. 20 characters minimum in length
   b. Complexity enabled

c. Minimum age of 1 day
d. 24 passwords remembered.

2. Domain Users
   a. 14 characters minimum in length
   b. Complexity enabled
   c. Minimum age of 1 day
   d. 12-24 passwords remembered.

PASSWORD DELETION:

All accounts and passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

1. When a user retires, quits, is reassigned, released, dismissed, etc.
2. Default passwords shall be changed immediately on all equipment.
3. Contractor accounts, when no longer needed to perform their duties.

PASSWORD PROTECTION STANDARDS:

Do not use your User ID as your password. Do not share passwords with anyone, including administrative assistants. All passwords are to be treated as sensitive, confidential information.

Here is a list of "do not's"

1. Don't reveal a password over the phone to anyone
2. Don't reveal a password in a mail message
3. Don't reveal a password to your supervisor
4. Don' talk about a password in front of others
5. Don't hint at the format of a password (e.g., "dog's name")
6. Don't reveal a password on questionnaires or security forms
7. Don't share a password with family members
8. Don't reveal a password to a co-worker while on vacation
9. Don't use the "Remember Password" feature of applications
10. Don't write passwords down and store them anywhere in your office.
11. Don't store passwords in a file on ANY computer system unencrypted.

REMOTE USERS

Access to Burrell networks via remote access is to be controlled by using a Virtual Private Network in which a password and user id are required. VPN must be accessed only on a company device and not a user's personal device.

6. Reports/Charts/Forms/Attachments/Cross References

7. Maintenance

Reviewed annually by CIO and IT Director

8. Signature

Approved by	2.1.2026
CIO	Date

9. Distribution List

Internal

10. Revision History

Revision Date	Subsection #	Summary of Changes	New/Cancellation/ Replacement Procedure? (if applicable)	Approval Date
2.1.2026		Reviewed		2.18.2026