Methodist College UnityPoint Health	Page # 1 of 4	Section: A	Policy #: A-68
	Approval: Dr. K. Q A. J		Date: 11/2014 Review by: 11/2017
	Date Revised: 11/2014		
	Policy/Revision Submitted by: Dr. Matthew Hertzog		

SUBJECT: **User ID and Password Security**

I. POLICY:

User IDs and Passwords are required to access the College and UnityPoint Health information system resources in order to ensure access is limited to authorized users. Users are responsible for maintaining the confidentiality of their passwords.

II. GENERAL INFORMATION:

BACKGROUND: The purpose of this policy is to:

1. Reduce the possibility of unauthorized access to College information systems.
2. Establish guidelines for creating and maintaining secure passwords.
3. Provide a uniform method for the creation and assignment of User IDs.
4. Create an accountability framework for College computer users.

This policy does not address how access to College and UnityPoint Health information systems will be granted. See Policy A.IT.04, Information Systems Access.

PROCEDURES:

1. Definitions.

   1.1 Password. A confidential sequence of characters used to authenticate an individual's identity or authorize access to data.

   1.2 User ID. A unique code or string of characters used to identify a specific user.

2. User Accountability and Responsibilities.

   2.1 The combination of User ID/Password is the equivalent of a user's legal signature and must not be disclosed to anyone, or the use of the combination permitted by anyone, other than the user to whom it is assigned.

2.2 Users are responsible and accountable for all activities performed under their User IDs.

2.3 Users must not attempt to learn or use another's User ID/Password.

2.4 Users must not access or attempt to access any computer system using another's User ID/Password.

2.5 Users are responsible for password-protecting files containing confidential or sensitive information (e.g. patient, student, financial, or employee information) that reside on their personal or shared directories.

2.6 Users shall not write, produce, run or possess any software designed to search and/or disclose Passwords.

3. Password Composition and Security.

3.1 Passwords must be a minimum of six characters in length for all information systems where possible.

3.2 Passwords should consist of a combination of alpha and numeric characters for all information systems where possible.

3.3 Passwords should not consist of repeating characters (e.g. 111111 or abababab), User IDs, birth dates, employee or social security number, telephone number, common character sequences (e.g. 123456 or abcdef), common words found in the dictionary or names of spouse, parent, children or pet.

3.4 Examples of good Passwords:

3.4.1 Two small words joined with a special character or number (e.g. dog#house or dog8house).

3.4.2 Words with numbers in place of vowels (e.g. d9gh97s3).

3.4.3 Using the first letters of a sentence, song or book title, or poem (e.g. I love to shop the Mall of America becomes Il2stMoA).

3.5 Passwords must expire at least every 180 days. If Passwords do not expire automatically, users are responsible for manually refreshing the passwords at least every 180 days.

3.6 New Passwords must be unique; reuse of old passwords is not permitted.

3.7 The College's IT department may assist users with password-related issues upon identification verification.

3.7.1 The College's IT department will only reset forgotten Passwords to a temporary Password. The user is required to change the Password once the system is accessed.

3.8 If unauthorized disclosure of a password is suspected, contact the College's IT department immediately for assistance with resetting the password.

3.9 Passwords should not be written down and stored in locations where another person might discover them (i.e. stuck to monitor, under keyboard, or desk drawer).

3.10 System default or temporary passwords must be changed the first time the system is accessed.

4. User ID Composition and Security.

4.1 User IDs must be unique for each user.

4.2 User IDs will not be renamed. If a user wants to change their User ID, they must submit a written request to the College's IT department. IT will create a new account and disable the old account. Requests for changes to user information associated with the User ID (i.e. name, title, department, etc.) should be submitted to the College's IT department via email and shall be considered on a user-by-user basis.

4.3 User IDs will be disabled after 120 days of inactivity. Supervisors must contact the College's Director of Human Resources to re-activate their User ID. The Director of HR will then notify the College's Director of Information Technology concerning re-enabling of the user's account.

4.4 User IDs will be disabled upon termination of employment or business contract. Termination notifications must be submitted to the College's Director of Human Resources. The Director of HR will then notify the College's Director of Information Technology concerning the disabling of the user's account.

4.5 Unless the College's Information Technology Department receives instructions to the contrary, 30 days after the Active Directory User ID has been disabled, it will be deleted and all files, including emails, held in the user's home directory and email account will be purged.

4.6 It is the responsibility of the department manager to notify IT of an employee's leave of absence that extends beyond 120 days.

4.7 After three unsuccessful log-on attempts, the User ID will be locked, and the user will be required to call the College's IT department to have the User ID unlocked upon identification verification.

5. Generic User IDs.

5.1 No generic user IDs will be provided to any temporary employee. Exceptions to this policy need to be generated through the College's Director of Human Resources.

6. Vendor Supported Systems.

6.1 Information systems that are not under the direct control of the IT Department are required to adhere to the standards set forth in this policy. A security administrator must be designated, whose responsibilities include assigning, changing, and removing User ID/Password authorizations.

6.2 Individually assigned User IDs/Passwords are required to access all confidential information systems.

7. Policy Violations.

7.1 Violations of this policy may result in disciplinary actions at the department level, immediate revocation of system access, and/or termination of employment or business contract.

7.2 Any suspected violations of this policy should be reported to the appropriate management the College's Director of Information Technology.