MARSHALL UNIVERSITY INFORMATION TECHNOLOGY COUNCIL

Procedure ITP-23

Password Standard for Administrative Systems

1. General Information:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password can result in the compromise of institutional information and the network. The purpose of this document is to establish a standard for the creation and maintenance of secure passwords used for access to administrative systems, to provide guidance in the baseline configuration account management and authentication systems, and to protect resources from unauthorized access.

1.1. Scope:

All Marshall University employees (including any contractor, vendor or auxiliary persons with access to Marshall University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. Strong password protection is especially critical for personnel who have or are responsible for an account or any form of access that supports or requires a password.

1.2. Authority: Information Technology Advisory Council

1.3. Passage Date: October 16, 2009; Revised Date: November 18, 2010; Recent Revision: July 30, 2018

1.4. Effective Date: 4/8/2019

1.5. Controlling over:

Passwords used for access to Marshall University Administrative Systems. Administrative systems are defined as information technology systems containing information resources which are required to conduct business in a timely and effective manner. These resources include financial, personnel, student, alumni, communication, identity, and physical resources data. Systems include but are not limited to Banner, Argos, muBERT, Active Directory.

2. General:

Account holders are responsible for the integrity and secrecy of their chosen passwords. Common security and privacy incidents can be avoided when choosing a strong password and adhering to regular password maintenance practices.

Increased complexity of password security controls shall be applied appropriate to the access privileges assigned to the user account and the sensitivity of the data being accessed (e.g. system user, system manager, system administrator).

Account passwords for use in administrative systems at Marshall University shall be created according to the following standards:

2.1. Password minimum length:

A password must be no fewer than eight (8) characters. Use of "Pass Phrases" (e.g. a password comprised of a short, memorable sentence instead of use of a single dictionary word) are strongly encouraged.

2.2. Composition & Complexity:

Passwords shall be composed in the following manner:

2.2.1. Must include at least one (1) character from each of these three (3) classes:

2.2.1.1. lowercase letters,

2.2.1.2. uppercase letters,

2.2.1.3. numerals, punctuation/special characters (for example, #, |, $, % and spaces). Note: some administrative systems do not support 'punctuation/special characters' in their password strings. In these cases, password length and complexity shall be increased to sufficiently reduce the risk of the password being easily guessed.

2.2.2. Must not use only a single common dictionary word, well-known or predictable phrases.

2.2.3. Must not match the same MUNet ID or display name of the account holder.

2.2.4. Must never be reused with non-University services.

Examples	Poor	Good
Must include 3 types of characters, do not use single dictionary word	rabbit, RABBIT	Run_Rabbit_Run
Must not use well-known passwords, predictable phrases or easily found information (e.g. off your social medial page)	Monkey123, P@ssw0rd, WeAreMarshall!, favorite sports team, kids or pets names	Monkey-Tree-Banana!, .Easy2TypePassword. ,
Must not patch your MUNet ID or display name – e.g. smith123, Jane Smith	Smith123, Jane_Smith	*Be more creative. Use something other than simply a person's username or display name.*
Must not reuse Marshall password anywhere else	Using the same password everywhere	*Marshall password is only used at Marshall*

Password Idea Starters:
* Think of a meaningful poem, lyric or quote. Take the first character of each word and write those down, maybe adding in some numbers or punctuation.
"*To be or not to be: that is the question*." = Tbontb:titq!
Result: a 12 character password that perhaps only has meaning for you and written down, simply looks like gibberish.
*Make up a bogus e-mail address with something familiar to you.
Snoopy@Woodstock.com
Result: Wow, a 20-character password!
*Music, science or foreign language examples – create a password based on musical notation or chord progression, a chemistry or mathematical formula or some unique phrase or expression not easily/directly translated into English. *Use your imagination*.

2.3. Password aging:

Password aging must be enabled to reduce the risk associated with account sharing and to assist in the process of identity management. Attempts to login using an expired password will fail.

2.3.1. *General user accounts* which have been granted access to an administrative system must change their password at least once every 180 days;

2.3.2. *Systems administrator account* are those user accounts which have been assigned elevated administrative access and are designated by the '-A' suffix – e.g. Smith123-A – and will have a password expiration of 90 days;

2.3.3. *Password Aging Exceptions* are granted to accounts configured to use multi-factor-authentication, and application service accounts which are used for non-interactive authentication.

2.3.4. Account Lockout: an account will be locked after five (5) failed logon attempts. This is to deter password guessing (brute force) attacks. The lockout will reset (expire) after thirty (30) minutes.

2.3.5. Super User Accounts (e.g. ROOT, DBADMIN, Domain Admin) must be configured to use an increased level of security controls to ensure their usage is only by authorized individuals. These controls must include one or more of the following: increased minimum password length to fifteen (15) characters, alerting upon account use and password changes, and use of multi-factor authentication where supported.

2.3.6. Reuse of old passwords: Passwords which are reported as compromised must never be reused by the accountholder. Password history settings must be set to the maximum allowable value to discourage previous passwords reuse.

2.3.7. Multi-factor authentication: where available and supported by the application, MUNet accountholders will use multi-factor (2-step) authentication to minimize unauthorized usage of their account.

2.3.8. Consequences for non-compliance: (1) Attempts to create or change a password to one that does not meet the above parameters will result in rejection of the change to the password. (2) Accounts with expired passwords will be denied logon until the password is reset by a system administrator.

2.3.9. Security Auditing: Information Technology will review security logs periodically and will investigate instances when potential unauthorized access or other exceptions are discovered.