UTEP Standard 15: Passwords

15.1 Procedures. In order to preserve the security of UTEP Information Resources and Data, Strong Passwords must be used to control access to Information Resources. All Passwords must be constructed, implemented, and maintained according to the requirements of the UT System Identity Management Federation Member Operating Practices (MOP), UTS165, and applicable UTEP Policies, Standards, and/or Procedures governing Password management.

(a) When issuing or resetting a User Passwords, the User's identity must be vetted. This may include having the User provide their UTEP Identification Number and a combination of any two of the additional criteria listed below. If the individual cannot provide the information requested, they must come in person and present a State issued picture ID.

i. Date of Birth
ii. Home address
iii. Phone number
iv. Zip code

(b) All passwords, including initial passwords, must be constructed and implemented according to the following rules:

i. Your password must be between 8 and 20 characters in length;
ii. You may not re-use any of your last 4 passwords;
iii. Your password must contain letters (upper and lower case), numbers, and special characters. Special characters that are permitted are: **! @ # $ % $ & * ( ) - + = ,< > : ; “ ’** .
iv. Your password cannot contain any words found in a dictionary or common proper nouns of four letters or longer. In addition, common letter transpositions are not allowed (e.g., @ for a, ! for I, or zero for O);
v. Your password cannot contain your first or last name;
vi. Your password cannot contain your birthday in any form;
vii. Your password cannot contain your Social Security Number;
viii. Administrators must have a password that is a minimum of 17 characters.

(c) Passwords must be changed as follow:
i. All user-level passwords (e.g., email, web, computing devices, etc.) must be changed at least once a year.
ii. Administrator passwords must be changed at least every 90-Days or sooner if a suspected compromise exists, and

anytime a Team Member leaves. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user. Passwords must conform to the administrator-level requirements;

iii. If the security of an account or password is in doubt or is suspected of having been compromised, the password must be changed immediately; or

iv. Password cracking or guessing may be performed on a periodic or random basis by the Information Security Office or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

(d) When applicable, security tokens (i.e., Smartcard, RSA token, Miner GoldCard, ProxCard, etc.) must be returned on demand or upon termination of the relationship with UTEP;

(e) Computing devices must not be left unattended without enabling a password-protected screensaver or logging-off of the device.

i. Do not use the "Remember Password" feature of applications (e.g., MS Outlook, Eudora, mail applications, web browsers, remote access applications, instant messenger applications, Netscape, Skype, etc.).

ii. Do not write passwords down and store them anywhere in your office.

iii. Do not store unencrypted passwords in a file on ANY computer system or mobile device.

(f) Passwords must only be accessed by or visible to the authenticating User, device, or system.

i. HelpDesk password change procedures must include the following:

1. User's identity must be appropriately vetted prior to changing and providing the user the password;
2. Temporary password must comply with minimum password requirements herein; and
3. The user must change their password at first login.

(g) Passphrases. Passphrases are a sequence of words or other text (e.g., a sentence) that are used to control access to a computer system, program or data. Because passphrases are longer versions of a password it is, therefore, more secure. Passphrases are composed of multiple words or a sentence and are relatively long. They contain a combination of upper and lowercase letters, numbers, and special characters. All password rules apply to passphrases. An example of a passphrase is shown below:

Example Phrase: "**I walk to the UTEP Library every morning before school**"
Final Passphrase: **!w2tULeM#b4s**

15.2 Sharing. Users must not share or divulge to anyone Passwords or similar information, or devices used for identification and authorization purposes.

15.3 Related Policies, Standards, Procedures, Guidelines and Applicable Laws

- UTEP Information Resources Use and Security Policy
- Standard 2: Acceptable Use of Information Resources
- Standard 11: Safeguarding Data
- Texas Administrative Code 202
- UTS165 Information Resources Use and Security Policy
- Payment Card Industry Data Security Standard (PCI DSS)
- NIST Special Publication 800-171

15.4 Revision History

First Draft:	March 28, 2002
Revised:	April 3, 2002
Revised:	September 19, 2002
Revised:	April 7, 2003
Revised:	June 18, 2003
Revised:	August 4, 2006
Revised:	September 11, 2006
Revised:	July 26, 2011
Revised:	September 30, 2014
Revised:	December 9, 2016 – reflect annual user password change requirement
Revised:	May 1, 2017
Approved:	May 9, 2017 – align with UTS165 formatting Gerard D. Cochrane Jr., Chief Information Security Officer