Policy Title: Strong Password Requirement

Policy Type: Technology **New/revised:** Revised

Old Policy #: Strong Password Requirement

Approval level: ☐ Board of Trustees
☒ President
☐ Vice President
☐ Other (specify here)

Purpose: This guideline provides recommendations for password use and creation in order to better protect IT systems and data. The guideline should be followed by ETSU Faculty, staff, students, contractors, consultants, temporaries, guests, volunteers, and other workers including all personnel affiliated with third parties with access to ETSU technological resources protected by authentication.

Policy:

Password Use

1. Passwords are to be treated as sensitive and confidential information:
    a. Avoid writing your passwords down – including in emails, printed and electronic forms.
    b. Avoid hinting at the format of your passwords (i.e., "it uses my family name").
    c. Avoid mentioning your passwords where they may be overheard by others.
    d. Be aware of your surroundings when typing your password.
    e. Do not save your passwords onto a plain text file.
    f. Do not share your passwords with anyone - including IT staff, supervisors, administrative assistants, colleagues, friends, and family members.

***Note**: IT Staff will never ask for your password. If someone does ask for your password report it to the CISO.*

2. Create unique passwords for each of your accounts and websites.

***Note:** Password managers such a LastPass, Dashlane, KeePass, and others can help you generate unique and strong passwords. A password manager that automatically fills your login information on a website, could help you identify phishing and fake websites when the login information is not automatically populated. Also, if you use a password manager, use a strong passphrase to protect all your passwords. Finally, enable two-factor authentication when offered by the password manager or website.*

3. Enable the use of passwords on desktops, as well as mobile devices such as tablets, smart phones and laptops.
4. If someone demands to know your password, refer them to this document or have them contact the Chief Information Security Officer.
5. If you suspect that your password has been compromised, report it to the Chief Information Security Officer and change the password immediately.

6. Avoid reusing passwords or portions of a passphrase of a compromised account.

Password Creation

1. ETSU systems automatically enforce the use of complex passwords, require passwords to be changed on a periodic basis, prevent users from re-using passwords, and implement and enforce various other password controls that may make it challenging to select a complex and easy to remember password.

Use the following tips to create a password that is easy to remember, hard to guess, and compliant with ETSU requirements:

a. Use a passphrase, or multiple words as the basis for a strong password.
b. Use character substitution or the first letter of each word:
    i. **I Like This Policy** may become **1L1k3Th1$P0l1cy**
    ii. **I Already Know How To Create Strong Passwords**, may become **iAkH2CsP**
c. Start, end or add special characters, i.e. **1L1k3Th1$P0l1cy!**
d. Add some numbers if needed, i.e. **1L1k3Th1$2017P0l1cy!**
e. The <space>, <dash>, <underline>, or any other special character can be used to separate words in passphrases and add complexity, i.e.:

    D0 Y0u Hav3 Ch@ng3 4$5?
    Y0u_L00k_@_8it_:-(
    ---> My-S3cr3t-H3r3! <---

2. Avoid using the following in passwords or passphrases:
    a. Demographic information.
    b. Dictionary words, or common word misspelling.
    c. Computer names, account information, or sample passwords.
    d. Phone, social security, credit card, identification, or other financial numbers.
    e. Common and notable phrases, i.e. “to be or not to be”, “E=mc2”, etc.

3. Avoid using personal information in password reset questionnaires and password hints whenever possible. They could be easily found on social media or public records.
4. Attempting to collect, guess, crack, or obtain someone else’s password is a violation of University policies.
5. Sharing ETSU passwords and login information is also a violation of University policies.

This guideline applies to ETSU passwords used to log onto campus Windows workstations, Desire2Learn, ETSU email, Sherrod Library Services, and any other services that use ETSU authentication. It is good practice to extend these practices to safeguard personal accounts. Requests for assistance can be directed to the ITS Help Desk at itshelp@etsu.edu or 423-49-4648.

Notes:
Approved: Information Technology Governance Committee
Reviewed: February 2017

3/24/2017 – approved by the Board of Trustees.