EAST TENNESSEE STATE UNIVERSITY

Password Policy

Policy Effective Date: 3/24/2017 • **Policy Revised Effective Date:** 6/08/26
Procedures Effective Date: N/A • **Procedures Revised:** Insert

Policy Name: Password Policy

Policy Purpose

This policy specifies requirements for password use and creation in order to better protect information technology systems and data.

Applicability

This policy is applicable to students, employees, contractors, consultants, guests, volunteers, and all personnel affiliated with third parties with access to university technological resources protected by authentication.

Responsible Official, Office, and Interpretation

The Information Technology Services and Information Technology Council are responsible for the review and revision of this policy. For questions about this policy, please contact Information Technology Services. The Chief Information Officer in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Multifactor Authentication (MFA)

A cybersecurity process that requires users to provide two or more verification factors to gain access to secure resources and systems, where such factors generally include something the user knows (such as a password or PIN), something the user has (such as an authentication application or hardware token), or something the user is (such as a biometric or behavioral factor).

Shoulder Surfing

Observing another person's screen or keyboard input without authorization, typically to obtain sensitive information.

Trusted Device

A device that has been registered and recognized as belonging to an authorized user.

Policy Name: Password Policy

Policy

ETSU enforces password and passphrase requirements in accordance with industry best practices and the National Institute of Standards and Technology (NIST).

1. Password Creation.

ETSU systems automatically enforce password complexity requirements, require password changes when an account is compromised, prevent password reuse, and implement additional password controls designed to enhance account security. ETSU will restrict access to or disable credentials that are suspected or confirmed to be compromised. Protection of account credentials is a shared responsibility between ETSU and account holders.

Users must create unique passwords or passphrases for each system or account. ETSU recommends the use of password phrases consisting of multiple words that are easy to remember but difficult to guess (e.g., "3tropicalbliZZardsh@ppen"). To comply with security requirements imposed by regulations, contractual obligations and other governing authorities, ETSU electronically enforces password length and complexity requirements. These requirements are subject to change.

Users requiring assistance with the setup, reset or modification of Multifactor Authentication (MFA) mentions should contact the ITS Help Desk. During authentication to ETSU systems, users may be given the option to designate a device as a Trusted Device. A Trusted Device may be recognized as an additional authentication factor, which can reduce the frequency of MFA challenges. Only devices under the user's exclusive control may be designated as Trusted Devices. Shared or public devices must not be designated as Trusted Devices.

Users should not include the following in passwords and passphrases:

1.1.1. Demographic information;

1.1.2. A single dictionary word by itself (e.g., "electromagnetic") or a common misspelling (e.g., "mispronounication");

1.1.3. Computer names, initials, account information, or example passwords;

1.1.4. Phone numbers, Social Security numbers, credit card numbers, identification numbers, or other financial information;

1.1.5. Information commonly available through social media or public records (e.g., alma mater, pets, or children's names, etc.); and

1.1.6. Common or notable words, phrases, and keyboard patterns (e.g., password, dragon, trustno1, winteriscoming, letitgo, passw0rd, 123456, qwerty, asdfgh).

Passwords must avoid predictable character substitutions (e.g., P@ssw0rd, Adm1n).

Attempting to collect, guess, crack, or obtain another individual's password by any means, including social engineering, is strictly prohibited. Sharing ETSU passwords or login credentials with others is prohibited.

2. Password Use.

ETSU passwords and passphrases are considered sensitive, confidential information and must be protected accordingly. Users must to safeguard their credentials at all times.

2.1. Users must not write down, record, or store passwords in any unsecured form, including on paper, in emails, or in unencrypted electronic files.

2.2. Users must not store password hints or descriptions on websites, devices, or files that could reveal the password or its structure (e.g., "it uses my family name").

2.3. Users must not disclose passwords verbally or in any written or electronic form where they could be overheard, intercepted, or viewed by others.

2.4. Users must remain aware of their surroundings when entering passwords to prevent Shoulder Surfing.

2.5. Passwords must never be stored in plaintext or unencrypted files.

2.6. Password sharing is strictly prohibited. Users must not share their passwords or login credentials with any individual – including Information Technology Services (ITS) staff, supervisors, administrative assistants, colleagues, friends, or family members.

2.7. ITS staff will never request a user's password. Any such request must be reported to the ITS Chief Information Officer.

2.8. Use of a reputable password manager (e.g., LastPass, Dashlane, KeePass, or similar tools) is strongly encouraged to generate and store unique, complex passwords.

2.9. All University-owned and personal devices used to access University resources, including desktops, laptops, tablets, and mobile devices, must be protected with a password, PIN, or biometric authentication mechanism.

2.10. If a password is suspected or known to have been compromised, the user must change it immediately and report the incident to the ITS Help Desk.

2.11. Users must not reuse passwords or passphrase components from any compromised or expired account.

Policy Name: Password Policy

Procedures

N/A

Applicable Forms and Websites

National Institute of Standards and Technology

Authority and Revisions

Authority: N/A

Previous Policy: Strong Password Requirement

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational program and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the Policy Development and Rule Making Policy webpage.

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.