



Texas Wesleyan University Information & Communication Technology

Password Policy

Purpose

This policy outlines the handling, responsibilities, and scope of passwords for the Information Technology ICT resources of Texas Wesleyan University. This policy acts as an extension of ICT security policy for Texas Wesleyan University

Authority

This policy has full support of the Texas Wesleyan University senior staff and human resources department. The ICT manager administers the policy, which is currently effective for all Texas Wesleyan University, employees, students, and computer systems.

Mission

The ICT objective of Texas Wesleyan University is to enable employees and students to perform their tasks with technology that is in good operating condition while appropriately addressing the business needs and keeping information secure within our ICT resources.

The Texas Wesleyan University, password dilemma

Passwords are the entry point to our ICT resources. Protecting access to our resources is pivotal in ensuring that our systems remain secure. While we have not exploited, nor do we expect to be, we must be diligent in guarding access to our resources and protecting them from threats both inside and outside our organization.

Password handling

Passwords for all systems are subject to the following rules:

- No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes supervisors and personal assistants.
- No passwords are to be shared in order to “cover” for someone out of the office. Contact ICT, and ICT will gladly create a temporary account if there are resources you need to access.
- Passwords are not to be your name, address, date of birth, username, nickname, or any other term that could easily be guessed by someone who is familiar with you.
- Passwords are not to be displayed or concealed within your workspace.

Systems involved

The Texas Wesleyan University, password policy will address passwords for the following ICT systems with their rules:

- **Network and client operating systems:** Windows username and password. (Users will automatically be prompted at a login to change the password every **60 days**.)
- **Outlook/Exchange groupware:** Windows username and password. (Users will automatically be prompted at a login to change the password every **60 days**.)
- **Computer BIOS password:** Hardware-level access to your computer. (This password will not automatically change.)
- **WIN (Administrative System/Datatel):** WIN username and passwords. (Users will automatically be prompted at a login to change the password every **90 days**.)
- **WWW Accounts:** Credentials to external Web resources (These passwords are rarely changed **unless initiated by the user**. ICT has disabled the option for these credentials to be saved. [Internet Explorer password caching] on all Texas Wesleyan University computers.)

Password composition

The following systems systematically enforce password requirements:

- **Network and client operating systems (and Outlook):** Passwords must meet the following criteria:
 - Password may not contain all or part of the user's account name.
 - Password is at least eight characters long.
 - Passwords contains characters from three of the following four categories:
 - English uppercase characters (A...Z)
 - English lowercase characters (a...z)
 - Base 10 digits (0...9)
 - Nonalphanumeric (exclamation point [!], dollar sign [\$], pound sign [#], percent sign [%], etc.) – DO NOT use [/], [\]

Support

All Texas Wesleyan University users are to contact the ICT staff for password policy support; ICT welcomes your questions and suggestions and strives to keep our resources secure.

ICT department will not give passwords (Windows, WebCT, Novell, Track-It, WIN, Mailing, etc.) to users over the telephone. If a user needs to have a password reset, ICT will **Email** the new password and instructions to the user only. Requests for **Windows network passwords** must be handled **in person with proper ID**.

Administrative passwords

Administrative passwords are subject to stringent composition, frequent change, and limited access. This includes passwords for routers, switches, WAN links, firewalls, servers, Internet connections, administrative-level network operating system accounts, and any other ICT resource.

Password for administrative resources must meet the following criteria:

- Password is at least 10 characters long.
- Password contains mixed case.
- Password contains at least three nonalphanumeric characters.
- Password contains at least two numbers.

Responsibilities

ICT has the responsibility to enforce this policy, through systematic means and interaction with users.

Texas Wesleyan University, users are responsible for complying with this policy.

Continuance

This Policy is a living document and may be modified at any time by the ICT manager, the senior staff, or the human resources department.

Top 10 Information Security Tips

1. Have you recently changed your password?
2. Do you leave your computer unattended?
3. Is your password-protected screensaver active?
4. Do you regularly back-up critical data?
5. Do you have current software virus protection?
6. Do you use only properly licensed software?
7. Is removable media stored safely?
8. Have you destroyed out-of-date CDs & floppies?
9. Have you disabled auto-answer on your modem?
10. Have you reported a security risk to ICT this year?

Summary

This policy is designed to secure Texas Wesleyan University, resources. This enables Texas Wesleyan University, to achieve its strategic objectives. Full cooperation with this policy is appreciated so that all goals can be met in accordance with the strategic objectives.