



TULANE UNIVERSITY PASSWORD POLICY

Department: Technology Services	Policy Description: Password
Approved: 01-02-2008	Revised:
Effective Date: 01-03-2008	Policy Number: TS-002

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Tulane University's entire network. As such, all students, faculty, staff, alumni, retirees, and other University affiliates (including contractors and vendors with access to Tulane University systems) are responsible for selecting and securing their passwords as outlined below.

2.0 Purpose

This policy establishes conditions for use of, and requirements for appropriate security for the Tulane Access Account. These requirements are necessary to help ensure personal security and protect Tulane's business, research, and academic interests.

3.0 Description

The Tulane Account contains a User ID (or "username") and password combination that serves as the primary digital identity for faculty, staff, and students. It works in tandem with the Tulane Online Directory, which uses Lightweight Directory Access Protocol (LDAP), a standardized method for providing directory information, to provide the foundation for digital identity authentication (who you are) and authorization (what you have access to).

Your User ID is usually your first initial, followed by the first seven characters of your last name. This is the public part of your digital identity, viewable by others when you send an e-mail or fill out a Web form. If your User ID is jdoe, then your Tulane e-mail address is jdoe@tulane.edu

Your password functions as a "key" that enables you to access the University's many electronic resources. This is the private part of your digital identity. You should protect and guard your password as you would your personal bankcard and PIN. You should never share your password with anyone, write it down, or make it easy for someone to guess (or "crack").

The Tulane Account provides access to a wide range of Tulane Internet services such as e-mail, myTulane, Library resources, E-Academy, secured Web sites, VPN, and Tulane-access computing labs. You may need additional University accounts for other services, including access to systems such as TAMS, SIS, and Datastore.

The Tulane Account is managed by the Technology Services Information Security Office.

4.0 Scope

This policy applies to every person using a Tulane Account at any time or location. This includes all students, faculty, staff, alumni, retirees, and other University affiliates (including contractors and vendors with access to Tulane University systems).

5.0 Policy

General:

- Passwords for newly activated Tulane Accounts must be changed at first use. This ensures that only the person who has been assigned the account knows the password.
- Tulane Account passwords will expire once every 90 days.
- Old passwords cannot be reused for 365 days. You are encouraged to avoid reusing old passwords, at all, if possible. See [Password Creation Guidelines](#) for tips on creating a strong password that is both easy to remember but hard to “crack.”

Your Responsibilities:

- Create a strong password; see [Password Creation Guidelines](#) below.
- Change the password at least once every 90 days, or more frequently as needed. You are responsible for changing your password before it expires, to avoid disruption of access to Tulane services. See [Password Expiration](#) below for additional details.
- Safeguard the password. You should not write down or store the password on paper or on a computer system where others might acquire it. See [Password Protection Standard](#) for additional guidelines.
- Never share the password, even with a best friend, roommate, or relative.
- Reserve the Tulane Account User ID and password for Tulane University systems and services only. You should create a different username and password for external services such as stores, banks, music services, Web sites, personally owned computers, or other systems.
- Any use of the Tulane Account is assumed to be performed by the person assigned to that account. You are responsible for all activities associated with your account.

Password Expiration:

- You are encouraged to change your password before it expires, in order to avoid disruption of access to University services. Passwords can be changed at <http://psync.tulane.edu>. At the first access to the password changing program (<http://psync.tulane.edu>) you must provide two security questions.
- Two weeks before the password expires, an e-mail notification of the expiration date will be sent to you. This e-mail notification will be sent daily until the password is changed or expires. If the password has not been changed by expiration date, the account will be locked.
- If you allow your password to expire you will need the correct answers for the two security questions to unlock the account. If the answers to the security questions are incorrect, you must contact the Help Desk to reinstate your Tulane Account access.
- The password should be changed immediately if you believe that it has been compromised (for example, if there is a possibility that another person may have viewed or acquired the password).

6. Guidelines

A. Password Creation Guidelines:

The following password guidelines are based upon experience and common sense. The software used to change passwords will screen for most of these guidelines as an aid in creating secure passwords. This does not relieve a person of responsibility for creating and securing a good password.

- 1.0 The password must be at least six characters in length. (Longer is generally better.)
- 2.0 The password should not be a word in the dictionary
- 3.0 The password must be in mixed case (upper- and lower-case letters)
- 4.0 The password must contain at least one numeric character.
- 5.0 The password cannot be the same as the user ID.
- 6.0 Special characters may be used to strengthen the password. Examples of permitted special characters are \$, ! % ^ *
- 7.0 The password should not be information easily obtainable about you such as your license plate number, social security number, telephone number, or street address.

B. Password Protection Standards

We strongly suggest that you do not use the same password for Tulane University accounts as for other non-Tulane University access (e.g., personal ISP account,

trading, benefits, etc.). Where possible, do not use the same password for all of your Tulane accounts.

Do not share Tulane University passwords with anyone, including administrative assistants or secretaries. All passwords should be treated as sensitive and confidential.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an e-mail message
- Don't reveal a password to your supervisor
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Office.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Entourage, and Webmail).

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encrypting the passwords.

If you believe that your account or password has been compromised, report the incident to Information Security Office (security@tulane.edu) and change the password for the affected account.