Policy Title: Password Policies	**Policy Number:**
Date Issued: March 20, 2007	**Responsible Executive: Vice President of Information Technology**
Date Last Revised: February 7, 2019	**Responsible Office: Information Technology Services**

Password Policies

Policy Statement

Systems at Baylor University ("Baylor" or the "University") that require passwords will, where possible, adhere to minimum password standards. Passwords that are issued to individuals are not to be shared with others. Using or attempting to use passwords for which you are not expressly authorized is prohibited. All systems will, where possible, store and transmit passwords in an encrypted or otherwise secured format.

Reason for the Policy

Passwords are an important means of preventing unauthorized access to computers, systems, and information resources. With minimal effort, users can greatly increase the effort required by an unauthorized user to compromise systems or information.

Individuals/Entities Affected by this Policy

This policy applies to all active members of the University community, including faculty, staff, students, and affiliates, and to authorized visitors, guests, and others for whom a University technology resource or access to the network has been provided.

Exclusions

NONE

Related Documents and Forms

University Policies and Documents

Handling of Confidential Information
Technology Systems Usage Policy
Network Usage Policies
Server Security Policy
1. Password Policies

Forms and Tools

Forms and tools are available at www.baylor.edu/its/.

Definitions

These definitions apply to terms as they are used in this policy.

Password	A password is defined as a secret series of alpha-numeric characters that allow a user to access a computer, program, file, or other IT resource.

Contacts

Subject	Contact	Telephone	Office email/web site
Support	ITS Help Desk	254-710-4357	https://www.baylor.edu/its/index.php?id=44608

Responsibilities

ITS Chief Information Security Officer or Designee	Responsible for developing and implementing an information security program to ensure that University communications, systems, and assets are safeguarded from threats
Chief Information Officer or Designee	Responsible for ensuring the policy remains current and for managing the application of the policy

Principles

Minimum Standard Structure

The preferred minimum standards for passwords at Baylor:

1. Are at least ten (10) characters in length.
2. Must contain characters from at least three of the following four categories:

    - English lowercase letter (e.g. a, b, c),
    - English uppercase letter (e.g. A, B, C),
    - Number (e.g. 1, 2, 3), and
    - Special character (e.g. @, #, *).

3. Expire every 365 days. Bear ID and TRAX are credentials that currently incorporate this standard.

Passwords may also be set to expire if ITS Security detects abnormal login patterns.

Password Precautions/Suggestions:

1. Don’t share your password with others. Helpdesk and ITS personnel will not ask for your password.
2. Choose passwords that you will be able to remember.
3. If a password must be written down or otherwise recorded, please ensure that it is kept in a secure place.
4. Users must log out or lock computers or other resources when leaving the system or computer unaccompanied.

Enforcement

1. Where possible, standards will be enforced by the underlying systems.
2. ITS personnel may audit passwords. If a password is found that does not meet minimum requirements, the user will be notified and asked to change their password.
3. ITS personnel may audit other Baylor systems to ensure compliance with this policy.

Sanctions

Sanctions may include, but are not limited to, suspension of technology privileges, termination of employment, referral to Student Judicial Services, and/or criminal prosecution. For additional information, please reference the Technology Systems Usage Policy.