Password Policies

Policy:
Systems at Baylor 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.

Topic Listing:
Definition of a Password
Minimum Standard Structure
Password Precautions/Suggestions
Enforcement

Related Policies and Legislation:
Technology Systems Usage Policy BU-PP 025
Network Usage Policies
Server Security Policy

Contact:
ITS Help Desk 710-4357

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 Technology Systems Usage Policy BU-PP 025.

Date Created/Updated
March 20, 2007

Rationale:
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.

Definition of a Password:
A password is defined as a secret series of alpha-numeric characters that allow a user to access a computer, program,
Minimum Standard Structure
The preferred minimum standards for passwords at Baylor:

1. Are at least eight (8) 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 insure 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.

Last modified February 7, 2019