

Tennessee Tech University: Information Technology Services

Password Policy

The usernames and passwords assigned to people to access information are critical in the protection of both our constituents' privacy and the University's information assets.

The username and password is for the use of a single individual and should be known only to that individual¹. There are several ways to protect the password and, where it is practical, systems will enforce these methods. This is complicated by the fact that many applications authenticate the username and password to the central authentication authority of our Active Directory (TTU domain). Because of audit concerns, some applications that have provided either single-sign-on capabilities or shared authentication authority will now have a separate login.

¹ There are only a few exceptions to this rule where group logins have been authorized.

Passwords should be protected as shown below:

1. Create a strong password. The password should not be common words in the dictionary, part of the user's name or names of family members (including pets), birth dates, anniversary or other significant dates. The password should contain letters and numbers, if allowed. Be very careful with special characters like %, &, _, \$, /, \ since in some applications, these characters have special meaning and may actually make your password useless. The password should be at least 6 characters, 8 to 12 is suggested.
2. Do not write a password down where it can be found. If you have a large number of passwords, there are PDA and PC applications that will password protect and encrypt your password in a database. ITS can assist users with locating an appropriate application.
3. Do not share your password with anyone, including coworkers or supervisors. If someone needs access through your account for some legitimate reason, log him or her in yourself. If someone needs access in your absence, then a data share can be established for your office so that people within the office can share documents securely. For administrative systems, each person will have to be authorized individually.
4. Where it is practical, the application system will enforce the policy.
5. The requirements and setup of specific administrative applications will be covered in the operational standards for that application.

Password Standards and Procedures

Internet Native Banner (INB)

1. Faculty/Staff with regular access to INB must change their password every 90 days.
2. Faculty/Staff with privileged access to INB must change their password every 30 days.
3. INB login accounts will be locked after 5 consecutive password failures.
4. The INB password is a separate and distinct password from the Active Directory domain password (TTU password).
5. Luminis Single Sign-on Technology may not be used.

Self-Service Banner (SSB)

1. Faculty/Staff/Students with access to Self-Service Banner (SSB) must change their PIN every 180 days. When the PIN expires, the user will be asked to set a new PIN. If the user forgets his or her PIN, there is a security challenge question which will allow the user to reset his or her PIN.
2. The **SSB PIN** is a separate and distinct password from the **Active Directory domain password** (TTU password).

Oracle

1. Faculty/Staff with regular access to Oracle must change their password every 90 days. There is a 10-day grace period, starting with the first login after the password expires.
2. Faculty/Staff with **privileged** access to Oracle must change their password every 30 days. There is a 10-day grace period, starting with the first login after the password expires.

Special Logins

1. Special logins, such as schema owners, default Banner users, and other special users that are infrequently used will be changed manually every 90 days.

TTU Domain

1. TTU Domain passwords (authenticated against the Active Directory) must be changed every 90 days.

Summary

User Type	Login To	Password/PIN Change Frequency
Faculty/Staff	INB (Internet Native Banner) (Regular Access)	Every 90 days
Faculty/Staff	INB (Privileged Access)	Every 30 days
Faculty/Staff/Student	SSB (Self Service Banner)	Every 180 days
Faculty/Staff	Oracle (Regular Access)	Every 90 days
Faculty/Staff	Oracle (Privileged Access)	Every 30 days
Faculty/Staff/Student	TTU Domain/PC Lab Domain/Email	Every 90 days
Special Logins		Every 90 days

Approved by the ITC Committee
This policy becomes effective May 1, 2009.