

Sam Houston State University
A Member of The Texas State University System
Information Technology Services (IT@Sam)

User Accounts Password Policy: IT-02

Introduction:

All user accounts will be protected by effective passwords that are both strong and confidential. Strong passwords have at least a specified minimum number of characters, are a combination of alphabetic, numeric and special characters, and are not common dictionary words. Refer to the IT@SAM Guidelines for Creating a Secure Password for specific details. Account holders and system administrators, acting as account/password custodians, will protect the security of those passwords by managing passwords according to IT@SAM password procedures.

From the time a password update, the probability that a password has been compromised increases. This probability increases because of the risk of silent compromise. Silent Compromise includes situations where the password was entered (keystroke logger) and intercepted by someone with malicious intent without the user's knowledge.

Spammers can use legitimate account passwords to log in to our email system and send large amounts of spam. These incidents result in our authenticated outgoing mail servers being added to numerous black lists, and have a negative effect on the entire SHSU community. If you are not careful with your password, the harm you cause can be to the SHSU community, not just yourself.

Scope:

The SHSU User Accounts Password policy applies equally to all individuals granted access privileges to any Sam Houston State University information technology resources.

Policy Statement:

Users are held responsible for all activities associated with their computer accounts. As such, the strength and protection of the password is critical to prevent unauthorized activity. The integrity and secrecy of an individual's authentication credentials are key elements of that responsibility.

Account holders must:

1. Create a strong password.
2. Change the password as frequently as needed to ensure security for the resources computers, data, etc. under their control. As a matter of practice, IT@SAM requires changing passwords at least once per 180 days.
3. Safeguard their password. For example, individuals should not write down or store the password on paper or on a computer system where others might acquire it.
4. Never share their password, even with a best friend, roommate, or relative. We recognize there may be times when people need to have someone do

something on their behalf, when work is being delegated, and lack of access to an account might impede business. That said, you are still responsible for what is done under your credentials regardless of intent.

5. Never reuse your SHSU username and password for external services, whether they are related to SHSU business or of a personal nature.
6. Change your password immediately if you know or suspect that it has been compromised. Contact IT@SAM Client Services for further guidance and assistance if this occurs.

Individuals responsible for administering systems and tools on campus must:

1. Prevent or take steps to reduce the exposure of any clear text, unencrypted account passwords that SHSU applications, systems, or other services have received for purposes of authentication.
2. Never request that passwords be transmitted unencrypted. Of particular importance is that passwords never be sent via email.
3. Coordinate with IT@SAM regarding their password procedures.

As security and privacy risks evolve, password standards need to evolve to meet those risks. The IT@SAM account password standard establishes requirements for:

1. Password minimum length
2. Password composition
3. Password aging
4. Reuse of old passwords

At initial account creation, a password is selected and tested against the current standards. IT@SAM may notify account holders of potentially weak or out of standard passwords based on IT@SAM's records of when a particular password was last changed.

Use of an encrypted password storage application is acceptable although extreme care must be taken to protect access to that application.

Related Policies, References and Attachments:

An index of approved IT@SAM policies, review dates, reference materials, legal compliance guidelines, policy enforcement and general definitions are available in the IT-00 Policy Compliance Document. The collection of Sam Houston State University Information Technology policies and procedures are available online through the SHSU Policy link from the SHSU.edu homepage.

Reviewed by: Mark C. Adams, Associate VP for Information Technology, May 15, 2011
Approved by: President's Cabinet, June 27, 2011
Next Review: November 1, 2014