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

User Accounts Password Policy: IT-02

PURPOSE:

All user accounts will be protected by passwords that are both strong and confidential. Users will protect the security of those passwords by managing passwords according to IT@Sam password procedures.

System and Application Administrators will ensure account passwords are secured using industry best practices.

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:

Users are responsible for what is accessed, downloaded, or created under their credentials regardless of intent. A non-authorized person can cause loss of information confidentiality, integrity and availability that may result in liability, loss of trust, or embarrassment to SHSU.

Account holders responsibilities:

1. Must create a strong password and protect it.
2. Password must have a minimum length of six (6) alphanumeric characters.
3. Password must contain a mix of upper case, lower case and numeric characters or special characters (!@#%^&*+=?/~';:,<>|\).
4. Passwords must not be easy to guess, for instance, they should not include part of your social security number, your birth date, your nickname, etc.
5. Passwords must not be easily accessible to others (e.g. posted on monitors, under keyboards).
6. Computing devices must not be left unattended without locking or logging off of the device.
7. Stored passwords must be encrypted.
8. SHSU username and password should not be used for external services (e.g. LinkedIn, Facebook or Twitter).
9. Users should never share their password with anyone, including family, supervisors, co-workers and IT@Sam personnel.
10. Users will be required to change passwords at least once per 180 days.

11. If you know or suspect that your account has been compromised, change your password immediately and contact IT@Sam Service Desk for further guidance and assistance.

12. It IT@Sam suspects your account has been compromised, your account will be deactivated and you will be contacted immediately.

Any individuals responsible for managing passwords 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. Never circumvent this password policy for the sake of ease of use.
4. Coordinate with IT@Sam regarding password procedures.

Detailed information and instructions for password management can be found on the SHSU website in the New Employee Technology Orientation training booklet. http://www.shsu.edu/~ucs_www/docs/TrainingBooklet.pdf

Related Policies, References and Attachments:

An index of approved IT@Sam policies can be found on the SHSU Information Technology Services Policies website at http://www.shsu.edu/intranet/policies/information_technology_policies/index.html. Reference materials, legal compliance guidelines, and policy enforcement are available in the IT-00 Policy Compliance Document. The SHSU Information Security Program and SHSU Information Security User Guide are also available on the Information Technology Services Policies website.

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