TEXAS STATE TECHNICAL COLLEGE
INFORMATION TECHNOLOGY OPERATING STANDARD

No. GA.5.1.1	**Page 1 of 2**	**Effective Date: 4/11/13**
TITLE:	**Password Use and Management for Information Resources**	
AUTHORITY:	**System Operating Standard GA 5.1**	
APPROVED BY:	**Management Council**	**Date: 4/11/13**

STATUS: Approved by MC 4/11/13

HISTORICAL STATUS: Proposed 4/2013

INTRODUCTION:
User authentication is a means to control access to an Information Resource. Controlling access is necessary for any Information Resource. Access by a non-authorized entity can result in loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to TSTC.

PURPOSE:
The purpose of the TSTC Password Standard is to establish the rules for the creation, distribution, safeguarding, and termination of TSTC user authentication mechanisms.

AUDIENCE:
The TSTC Password Standard applies to all individuals who use any TSTC information resource.

DEFINITIONS:
Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus and the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information on those resources

Information Security Coordinator (ISC): Responsible for administering the information security functions within the agency. The ISC is the agency's internal and external point of contact for all information security matters.

Office of Information Technology (OIT): The name of the agency department responsible for computers, networking and data management.

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny access to private or shared TSTC data.

PASSWORD STANDARD:

- All passwords must be constructed and implemented according to the specific requirements as set forth in individual application governance document(s). If no governance document exists the password will be constructed in the following manner: At least 8 characters long and must be a combination of letters and numbers.
- User passwords stored in enterprise systems must be encrypted or protected from disclosure except to the user.
- User account passwords must not be divulged to anyone. TSTC OIT and contractors will not ask for user account passwords.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with TSTC.
- If the security of a password is in doubt, the password must be changed immediately.
- Anyone given access to TSTC owned information resources will not circumvent password entry with auto logon, application remembering, embedded scripts hardcoded passwords in client software, or web browser credential remembering feature. Exceptions may be made for specific applications (like automated backup) with the approval of the TSTC ISC. In order for an exception to be approved there must be a procedure to change the passwords.
- Computing devices must not be left unattended without enabling a password-protected screensaver. The user may meet this requirement by logging off of the device.
- OIT Helpdesk password change procedures must include the following:
    1. authenticate the user to the helpdesk before changing password
    2. the user must change password at first login
- In the event passwords are openly discovered, the following steps must be taken:
    1. Take control of the passwords and protect them
    2. Report the discovery to the OIT Help Desk
    3. Transfer the passwords to an authorized person as directed by the TSTC ISC.

Any legacy application in use prior to the acceptance of this standard that cannot comply with this standard will be subject to a life cycle review. Based on that review, recommendations will be made to secure the application with reasonable means. The TSTC ISC will document the resulting action.

DISCIPLINARY ACTIONS:

Non-compliance with established standards and rules and procedures will subject the employee to a range of corrective actions pursuant to SOS HR.2.4.1 Employee Corrective Action.