# TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

**HSCEP OP:** 56.01, 1.4.12 **PASSWORD/AUTHENTICATION**

**PURPOSE:** The purpose of this Texas Tech University Health Sciences Center El Paso (TTUHSC El Paso) Operating Policy and Procedure (HSCEP OP) is to establish guidelines for setup and maintenance of user authentication measures.

**REVIEW:** This HSCEP OP will be reviewed on annually by the Information Security Officer and approved by the Chief Information Officer (CIO)

**POLICY/PROCEDURE:**

In accordance with Texas Administrative Code § 202.75 and Center for Internet Security (CIS) critical control catalog items, all TTUHSC El Paso computing systems shall require a login authentication process, whereby each user is identified and authenticated through their unique USER ID and/or account name. Access to the network and to applications is based on individual roles and determination of user access levels is the responsibility of the owners of the information or applications being accessed. All TTUHSC El Paso information resources shall be joined to the TTUHSC El Paso domain for authentication unless approved by the Information Security Officer for alternate authentication. All systems which support the option shall use centralized authentication via LDAPS, CAS, and similar technologies which leverage domain authentication. Texas Tech's primary authentication is through an account management system known as eRaider, which allows users to access the information resources available at the Health Sciences Center. Passwords for eRaider accounts follow industry best practices and must meet the following minimum requirements:

- Must be 9 - 25 alphanumeric characters
- Must contain upper & lower case characters
- Must contain a number
- Must NOT contain a number as the first or last character
- Must NOT be reused within a one year period

Recommendations

- Choose a password that is not easy to guess
- String together uncommon words
- NEVER share your password with anyone
- Use a different password for every site

Passwords must be changed every 180 days.

**Privileged Accounts**

- **Multifactor authentication must be implemented for access to privileged or administrative level accounts**

II. **System Identification/Logon Banner**

Any TTUHSC El Paso computing system that prompts the user for a login shall require an unauthorized access warning banner to be displayed. The unauthorized access warning banner must inform the user of the restrictions imposed on the system before access is attempted, thereby giving the user the opportunity to avoid violating any access restrictions. The HSCEP OP 56.01 Unauthorized Access Warning Banner must be prominently displayed each time a user attempts to access a server system, network terminal, and/or a restricted/secured web site and/or web page, specifically before the user can begin the login authentication process. The Unauthorized Access Warning Banner will be made part of the web site and/or web page preceding a restricted/secured web site and/or web page and must be displayed before a user enters the secured web site and/or web page. The user must also be made to acknowledge the warning either in the form of an icon or button stating “OK” or “I Accept” before they can proceed.

III. **Disclaimer Statement.** TTUHSC El Paso reserves the right to interpret, change, modify, amend or rescind any policy in whole or in part at any time without the consent of employees.