I. POLICY STATEMENT

User authentication is a means to control who has access to an information resource technology system. Controlling the access is necessary for any information resource technology. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to the University. These factors, or a combination of these factors, can be used to authenticate a user. Examples are:

1. Something you know- password, Personal Identification Number (PIN),

2. Something you have- Smartcard,

3. Something you are- fingerprint, iris scan, voice, or

4. A combination of factors- Smartcard and a PIN.

II. PURPOSE AND SCOPE

The purpose of the University Password Security Policy is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the University user authentication mechanisms. To the extent this policy conflicts with existing University policy, the existing policy is superseded by this policy. The University Password Policy applies equally to all individuals who use any of the University's information resources and technology.

III. DEFINITIONS

N/A

IV. POLICY PROVISIONS

1. All passwords, including initial passwords, must be constructed and implemented according to the following Office of Information Technology ("OIT") rules:

    1.1. Passwords must be routinely changed.

    1.2. Passwords must adhere to a minimum length as established by the University Information Security Officer ("ISO").

1.3. Passwords must be a combination of alpha and numeric characters.

1.4. Passwords must not be anything that can easily be tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.

1.5. Passwords must not be dictionary words or acronyms.

1.6. Password history must be kept to prevent the reuse of a password.

1.7. Stored passwords must be encrypted.

2. User account passwords must not be divulged to anyone. OIT and any University contractors will not ask for user account passwords.

3. Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with the University.

4. If the security of a password is in doubt, the password must be changed immediately.

5. Administrators must not circumvent the Password Security Policy for the sake of ease of use.

6. Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the University ISO. In order for an exception to be approved there must be a procedure to change the passwords.

7. Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.

8. OIT Helpdesk password change procedures must include the following:

8.1. Authenticate the user to the Helpdesk before changing the password,

8.2. Change to a strong password, and

8.3. The user must change password at first login.

9. In the event passwords are found or discovered, the following steps must be taken:

9.1. Take control of the passwords and protect them,

9.2. Report the discovery to the University Help Desk, and

9.3. Transfer the passwords to an authorized person as directed by the University ISO.

10. The ISO is authorized to enact Password Guidelines to assist users in developing passwords.

11. Disciplinary Action

Violation of this policy may result in immediate Disciplinary Action pursuant to University policy (MAPP 02.05.03 – Discipline and Termination Policy).

12. Applicable TSU Security Policy Standards

All individuals with authorized access to any TSU information resource and technology, including staff, faculty, students, consultants, contractors and volunteers, must adhere to all provisions of this policy, as well as applicable security standards included in the Security Standards Policy – MAPP 04.06.22). Applicable security standards include, but are not limited to:

- Security Standard 1
- Security Standard 2
- Security Standard 3 Security Standard 4
- Security Standard 5
- Security Standard 9
- Security Standard 16