1. GENERAL

Authentication refers to the process where a user verifies their identity (e.g., their username) by presenting one or more authentication factors: password, physical token (e.g., smartcard), fingerprint, etc. Authentication is a means to control who has access to an information resource. Controlling access is necessary for any information resource. The confidentiality, integrity, and availability of information can be lost when access is gained by a non-authorized entity. This, in turn, may result in loss of revenue, liability, loss of trust, or embarrassment to the University.

The purpose of the University Procedure is to establish the process for the creation, distribution, safeguarding, termination, and reclamation of the University’s user-authentication mechanisms.

2. APPLICABILITY

This University Procedure applies to all University information resources.

The purpose of the implementation of this University Procedure is to provide a set of measures that will mitigate information security risks associated with password authentication. There may also be other or additional measures that will provide appropriate mitigation of the risks. The assessment of potential risks and the application of appropriate mitigation measures are to be determined by the information resource owner or their designee.

Please also refer to Procedure 29.01.03.C2.25 “Exceptions from Risk Mitigation Measures.”

The intended audience is any University student, faculty, staff, employee, guest, or visitor that uses information resources requiring authentication.

3. DEFINITIONS

Please refer to University Procedure 29.01.03.C2.01 “Definitions” for definitions of commonly used terms. The terms defined below are specific to this Procedure.

IdP stands for identity provider, i.e., any service that stores account credentials (e.g., usernames and passwords) and provides authentication of users based on those
credentials. Examples of current University IdPs include Active Directory, Open LDAP, and Banner.

IdP Custodian is a person who manages an IdP and thus manages not only the stored identities, but also the processes whereby identities are created, modified, and disabled or deleted.

Password shall refer to any password that protects a University information resource or protects University data.

4. PROCEDURES
4.1. The IRM or his or her designee(s) shall issue password guidelines (“the password guidelines”) defining one or more classes of passwords and for each class so defined, detailing at least the following:

4.1.1. Password length (i.e., minimum and maximum password character lengths);

4.1.2. Password complexity (i.e., which character sets must be used in constructing a password);

4.1.3. Password expiration (i.e., amount of time since last successful password change after which the password expires);

4.1.4. Password lockout (i.e., how many invalid password attempts are permitted in a given amount of time before the account is locked and how long does the account remain locked);

4.1.5. Password history (i.e., keeping a record of prior password values so as to avoid password reuse), and;

4.1.6. The information resources to which this class of passwords applies.

4.2. In creating the password guidelines, the IRM or his or her designee(s) will consult existing password standards in the higher education community and the world. Also, the IRM or his or her designee(s) shall ensure that the password guidelines meet or exceed the following requirements:

4.2.1. Minimum password length is eight (8) characters.

4.2.2. Accounts will be locked after no more than seven (7) consecutive invalid password attempts.

4.2.3. Accounts locked by the mechanism described in 4.2.2. shall remain locked for at least ten (10) minutes.
4.3. IdP Custodians shall ensure that all passwords adhere to the appropriate password guidelines. User accounts with passwords that do not adhere to the password guidelines may be disabled by the IRM or his or her designees, or by the appropriate IdP Custodian.

4.4. A user shall not divulge any of their passwords to anyone without the express, prior approval of the IRM.

4.5. A user shall not access a University information resource with a password other than his or her own without the express, prior approval of the IRM.

4.6. If a user doubts the security of any of their passwords, the user shall change the password(s) immediately.

4.7. A first user shall not ask a second user for the second user’s password without the express, prior approval of the IRM.

4.8. If a first user comes into possession of a second user’s password, the first user shall notify the IT Department immediately. An exception to this rule is IdP Custodians creating one-time passwords for their users.

4.9. If a first user knows or reasonably should know that a second user’s password has been compromised (e.g., the second user shared it with a third user), then the first user shall notify the IT Department immediately.

4.10. Users shall not store the plaintext of a password. Passwords must be encrypted before being stored.

4.11. Users shall not transmit unencrypted passwords across a network.

4.12. Users must return security tokens (e.g., Smartcard) on demand of a supervisor or the token’s Custodian, or upon termination of the relationship with the University.

4.13. IdP Custodians shall only replace forgotten passwords, not reissue them.

4.14. Users must not circumvent this University Procedure for the sake of ease of use.

4.15. Users should not circumvent password entry with auto logon, embedded scripts, or hard-coded passwords in client software.

4.15.1 Exceptions may be made for specific applications, such as automated backup, with the approval of the IRM.

4.15.2 In order for an exception to be approved there must be a documented procedure for changing the password(s).

4.15.3 Exceptions and associated risk reduction countermeasures must be documented during the information resource’s annual risk assessment.
4.16. Users shall not circumvent password entry with application remembering, e.g., a browser remembering a user’s password for future re-use.

4.17. Users shall not leave computing devices unattended without enabling a password-protected screensaver or logging off of the device.

4.18. Custodian of systems providing mission critical services or containing Sensitive Information shall configure those systems to automatically initiate a password-protected screensaver or log a user off after 15 minutes of inactivity.

4.19. Custodians shall configure authentication mechanisms to log successful and failed authentication activity.

4.20. IdP Custodians shall ensure that password reset procedures include the following steps:

4.20.1. authenticate the user before changing password;

4.20.2. change to a strong one-time password, and;

4.20.3. user must change password at first login.

4.21. Users shall not use password-cracking utilities without the express, prior approval of the IRM or his or her designee(s).

4.21.1 Password-cracking utilities should be configured so that they do not reveal the actual password being evaluated, regardless of whether that passwords fails or meets the password guidelines.

4.21.2 Users whose passwords do not meet the password guidelines shall be notified via their University e-mail account.

6. CONSEQUENCES FOR VIOLATIONS

All University employees to include staff, tenured and non-tenured faculty, graduate assistants, student workers, interns, guests, volunteers, and probationary, temporary, or wage employees as well as contractors, consultants, and vendors required to adhere to this university procedure may be subject to criminal, civil, or disciplinary actions consistent with federal and state laws, system policies, and university rules.

Individuals found in violation of this University Procedure are subject to loss of access privileges to University information resources (e.g. servers, workstations, email, etc). In addition, contracts associated with contractors, consultants, or vendors are subject to review and possible termination. Any device, system, or software found in violation of this procedure may be confiscated and temporarily stored by the Information Resources Manager or a representative of the office.
Additional guidance may be found, but is not limited to, the following policies and rules.

- **Texas A&M System Policy**
  - 01.03 Appointing Power and Terms and Conditions of Employment
  - 07.01 Ethics Policy, TAMUS Employees
  - 32.02 Discipline and Dismissal of Employees
  - 32.02.02 Discipline and Dismissal Procedure for Nonfaculty Employees
  - 33 Employment, Standards of Conduct

- **Texas A&M University-Corpus Christi Rule**
  - 12.01.99.C3 Faculty Dismissals, Administrative Leave, Non-Reappointments and Terminal Appointments
  - 13.02.99.C1 Student Disciplinary Proceedings

- **Texas A&M University – Corpus Christi Procedures**
  - Procedure 29.01.03.C2.03 Management of User Accounts
  - Procedure 29.01.03.C2.04 Administrator/Special Access

Contact for Interpretation: Office of Information Security

Office of Responsibility: Office of the Associate VP for Information Technology and CIO