

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.15 Password

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

User authentication is a means to control who has access to an information resource system. Controlling the 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. There are several ways to authenticate a user. Examples are: password, university identification number (UIN), Smartcard, fingerprint, iris scan, or voice recognition.

The purpose of the university password/authentication procedure is to establish the process for the creation, distribution, safeguarding, termination, and reclamation of the university 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. In accordance with Texas Administrative Code 202 - Information Security Standards, each department and/or resource owner may elect not to implement some or all of the risk mitigation measures provided in this university procedure based on information security risk management decisions and business functions. Such risk management decisions must be documented in the annual security assessment report (See University Rule 21.01.06.C2 Security of Electronic Information Resources).

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 21.01.06.C2.01 Definitions.

4. PASSWORD GUIDELINES

- Workstation passwords must be changed at least every 90 to 180 days.

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- Resource custodian passwords must be changed every 90 days.
- All passwords on systems containing mission critical services or sensitive information must be changed every 90 days.
- Passwords must have a minimum length of eight alphanumeric characters
- Passwords must contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters must not be at the beginning or the end of the password. Special characters should be included in the password where the computing system permits. The special characters are (!@#\$\$%^&* _+=~/~`::;<>|\
 - Combine short, unrelated words with numbers or special characters. For example: eAt42peN.
 - Make the password difficult to guess but easy to remember.
 - Substitute numbers or special characters for letters. (But do not just substitute).
 - For example:
 - livefish - is a bad password.
 - L1veF1sh - is better and satisfies the rules, but setting a pattern of first letter capitalized, and i's substituted by 1's can be guessed.
 - !!v3f1Sh - is far better, the capitalization and substitution of characters is not predictable
- Passwords must not be easy to guess and they must not be:
 - your username
 - your employee number
 - your name
 - family member names
 - your nickname
 - your social security number
 - your birthday
 - your license plate number
 - your pet's name
 - your address
 - your phone number
 - the name of your town or city
 - the name of your department
 - street names
 - makes or models of vehicles
 - slang words
 - obscenities
 - technical terms
 - school names, school mascot, or school slogans
 - any information about you that is known or is easy to learn (favorite - food, color, sport, etc.)
 - any popular acronyms
 - words that appear in a dictionary
 - the reverse of any of the above

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- Passwords must not be reused for a period of one year
- Passwords must not be shared with anyone
- Passwords must be treated as confidential information

5. PROCEDURES

- 5.1. All passwords protecting university information resources must adhere to the password guidelines as set forth in this procedure. User accounts that do not adhere to these guidelines can be disabled by the information security representatives or departmental information security custodians.
- 5.2. Resource custodians are permitted to utilize password-cracking utilities to test passwords within their defined areas of responsibility after notification of the specific department's manager or the Information Resources Manager.
 - (1) Password cracking utilities must be configured so that they do not reveal the actual password being evaluated whether they fail or meet the Password Guidelines.
 - (2) Users whose passwords do not meet Password Guidelines shall be notified via their university e-mail account.
- 5.3. Stored passwords must be encrypted.
- 5.4. User names and passwords being transmitted across the wired or wireless network must be encrypted.
- 5.5. Passwords must not be divulged to anyone. Media and Computer Services and Media and Computer Services contractors or other university employee shall not ask for user account passwords.
- 5.6. Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with the university.
- 5.7. If the security of a password is in doubt, the password must be changed immediately.
- 5.8. Forgotten passwords shall be replaced, not reissued.
- 5.9. Administrators must not circumvent this university procedure for the sake of ease of use.
- 5.10. Password entry must not be circumvented with auto logon, application remembering, embedded scripts, or hard-coded passwords in client software.

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- (1) Exceptions may be made for specific applications, such as automated backup, with the approval of the department manager.
 - (2) In order for an exception to be approved there must be a documented procedure for changing the password(s).
 - (3) Exceptions and associated risk reduction countermeasures must be documented during the information resource's annual risk assessment.
- 5.11. Computing devices must not be left unattended without enabling a password-protected screensaver or logging off of the device.
- 5.12. Systems providing mission critical services or containing Sensitive Information must be configured to automatically initiate a password-protected screensaver or log off after 15 minutes of inactivity.
- 5.13. Authentication mechanisms shall be configured to log successful and failed authentication activity.
- 5.14. Systems providing mission critical services or containing Sensitive Information must be configured to lock user and administrator account for a period of no less than 10 minutes after seven failed login attempts.
- 5.15. Media and Computer Services Helpdesk password change procedures must include the following:
- (1) authenticate the user to the helpdesk before changing password,
 - (2) change to a strong password, and
 - (3) user must change password at first login.
- 5.16. In the event written or stored passwords are found or discovered, the following steps must be taken:
- (1) take control of the passwords and protect them, and
 - (2) report the discovery to the department manager or Media and Computer Services Helpdesk.

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

UNIVERSITY PROCEDURES

TEXAS A&M UNIVERSITY-CORPUS CHRISTI

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

Contact for Interpretation: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration