29.01.99.K1.120 Password Standard Administrative Procedure

Effective: April 1, 2004
Revised: June 21, 2013
Revised: October 8, 2019
Next Scheduled Review: October 8, 2024

Introduction

User authentication is a means to control who has access to an information resource system. Controlling the access is necessary for any information resource. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue and trust, increase in liability and embarrassment to Texas A&M University-Kingsville (TAMUK).

Purpose

The purpose of this procedure is to establish the rules for the creation, distribution, safeguarding, termination, and reclamation of the TAMUK user authentication mechanisms.

Audience

This procedure applies to individuals who use any University information resource.

Password Procedure

1. All passwords must be constructed and implemented according to the following criteria:
    a. Passwords will expire after 180 days except for service accounts, root accounts and Windows administrator accounts.
    b. Passwords must meet the following complexity:
        i. must have a minimum length of eight (8) characters
        ii. must contain three of the following:
            1. upper case (A-Z)

2. lower case (a-z)
3. special character (! @ # $ % & * _ + = ? / ~ ` ; : , < > | \ )
4. numeral (0-9)

2. User account passwords must not be divulged or shared with anyone. iTech will not ask for user account passwords.
3. Password history must be kept for three (3) prior iterations to prevent the reuse of a password, if the system is capable.
    a. Passwords can only be changed once every 24 hours.
4. Stored passwords must be encrypted and not transmitted as plain text.
5. There shall be no more than five (5) consecutive failures before a user is locked out of an account for 30 minutes, when the system is capable.
6. If the security of an account/password is in doubt, the password must be changed immediately.
7. Administrators must not circumvent this Password Procedure for the sake of ease of use.
8. Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
9. Users should not circumvent password entry with auto logon.
10. Service account passwords for system-to-system interaction (e.g., backups, stored procedures) do not require a password change. Service account passwords must be at least 16 characters.
11. Linux root account and Windows administrator account passwords must be at least 16 characters.
    a. Linux root account and Windows administrator account passwords must be changed annually or when an authorized administrator no longer needs access.

Password Guidelines

---

1. Passwords must not be easy to guess and they:
    a. should not contain your Username
    b. should not contain your employee number
    c. should not contain your name
    d. should not contain family member names
    e. should not contain nickname
    f. should not contain your social security number
    g. should not contain your birthday
    h. should not contain your license plate number
    i. should not contain your pet's name
    j. should not contain your address
    k. should not contain your phone number

l. should not contain the name of your town or city
m. should not contain the name of your department

Disciplinary Actions

Violation of this procedure may result in disciplinary action up to and including termination for employees and temporaries; a termination of contract relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of students. Additionally, individuals are subject to loss of TAMUK Information Resources access privileges, civil, and criminal prosecution.

References

1. Computer Fraud and Abuse Act of 1986
2. Computer Security Act of 1987
3. DIR Practices for Protecting Information Resources Assets
4. DIR Standards Review and Recommendations Publications
5. The State of Texas Information Act
6. The State of Texas Penal Code, Chapters 33 and 33A
7. Texas Administrative Code, Chapter 202
8. Texas A&M University-Kingsville Acceptable Use Procedure 29.01.99.K1.010
9. Texas Government Code, Section 441
10. System Regulation 29.01.03 Electronic Information Services Access and Security

Contact Office

For More Information, Contact: iTech
MSC 185, 700 University Blvd., Kingsville, TX 78363-8202
Contact Phone: 361-593-2404