

**THE TEXAS A&M UNIVERSITY SYSTEM
HEALTH SCIENCE CENTER INTERNAL POLICIES**

29.01.03.Z1.02 Password

Approved September 1, 2010

Supplements System Regulation 29.01.03

1. GENERAL

1.1 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, liability, loss of trust, or embarrassment to Texas A&M University System Health Science Center (HSC).

Three factors, or a combination of these factors, can be used to authenticate a user. Examples are:

- Something you know – password, Personal Identification Number (PIN)
- Something you have – Smartcard
- Something you are – fingerprint, iris scan, voice
- A combination of factors – Smartcard and a PIN

1.2 Purpose

The purpose of the HSC Password Policy is to establish the standards for the creation, distribution, safeguarding, termination, and reclamation of the HSC user authentication mechanisms.

1.3 Audience

The HSC Password Policy applies equally to all individuals who use any HSC information resource.

1.4 Definitions

- **Information Resources (IR):** any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network

attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

- **Information Resources Manager (IRM):** Responsible to the State of Texas for management of the institution's information resources. The designation of an institution information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state institution's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the institution. If an institution does not designate an IRM, the title defaults to the institution's President, and the President is responsible for adhering to the duties and requirements of an IRM.
- **Information Security Officer (ISO):** Responsible to the executive management for administering the information security functions within the institution. The ISO is the institution's internal and external point of contact for all information security matters.
- **Office of Information Technology (OIT):** The name of the institution department responsible for computers, networking and data management.
- **Password:** A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.
- **Strong Passwords:** A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.

2. PASSWORDS

2.1 All passwords, including initial passwords, must be constructed and implemented according to the following HSC IR standards:

- it must be routinely changed
- it must adhere to a minimum length as established by HSC OIT
- it must be a combination of alpha and numeric characters
- it must not be anything that can easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
- it must not be dictionary words or acronyms
- password history must be kept to prevent the reuse of a password

- 2.2 Stored passwords must be encrypted.
- 2.3 User account passwords must not be divulged to anyone. HSC OIT and OIT contractors will not ask for user account passwords.
- 2.4 Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with HSC.
- 2.5 If the security of a password is in doubt, the password must be changed immediately.
- 2.6 Administrators must not circumvent the Password Policy for the sake of ease of use.
- 2.7 Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software. Exceptions may be made for specific applications (like automated backup) with the approval of the HSC ISO. In order for an exception to be approved there must be a procedure to change the passwords.
- 2.8 Computing devices must not be left unattended without enabling a password protected screensaver or logging off of the device.
- 2.9 OIT Help Desk password change procedures must include the following:
 - Authenticate the user to the helpdesk before changing password
 - Change to a strong password
 - The user must change password at first login
- 2.10 In the event passwords are found or discovered, the following steps must be taken:
 - Take control of the found passwords and protect them
 - Report the discovery to the HSC OIT Help Desk
 - Transfer the passwords to an authorized person as directed by the HSC ISO.

3. PASSWORD GUIDELINES

- 3.1 Passwords should be changed at least every 180 days.
- 3.2 Passwords should have a minimum length of 8 alphanumeric characters.
- 3.3 Passwords should contain a mix of upper and lower case characters and have at least 2 numeric characters. The numeric characters should 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 (!@#\$%^&* _+=~/~`';:, <>|\).
- 3.4 Passwords must not be easy to guess and they:
 - Should not be your Username
 - Should not be your employee number
 - Should not be your name

- Should not be family member names
- Should not be your nickname
- Should not be your social security number
- Should not be your birthday
- Should not be your license plate number
- Should not be your pet's name
- Should not be your address
- Should not be your phone number
- Should not be the name of your town or city
- Should not be the name of your department
- Should not be street names
- Should not be makes or models of vehicles
- Should not be slang words
- Should not be obscenities
- Should not be technical terms
- Should not be school names, school mascot, or school slogans
- Should not be any information about you that is known or is easy to learn (favorite - food, color, sport, etc.)
- Should not be any popular acronyms
- Should not be words that appear in a dictionary
- Should not be the reverse of any of the above

3.5 Passwords should not be reused for a period of one year.

3.6 Passwords must not be shared with anyone.

3.7 Passwords must be treated as confidential information.

4. CREATING A STRONG PASSWORD

4.1 Combine short, unrelated words with numbers or special characters. For example:
eAt42peN

4.2 Make the password difficult to guess but easy to remember.

4.3 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 1st letter capitalized, and i's substituted by l's can be guessed
- !v3f1Sh - is far better, the capitalization and substitution of characters is not predictable

5. DISCIPLINARY ACTIONS

Violation of this policy may result in disciplinary action which may include termination for employees and temporary workers; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of HSC information resources access privileges, civil, and criminal prosecution

OFFICE OF RESPONSIBILITY

Vice President for Information Technology and Chief Information Officer