Texas Health Resources

Policy Name: Password Management	
Policy Owner: Information Security Governance Council	**Effective Date:** 08/29/2023
Approved By: System Performance Committee	**Last Reviewed Date:** 08/29/2023
Page 1 of 9	

1.0 Scope:

1.1 Applicable Entities:
This policy applies to:

- Texas Health Resources (Texas Health) and its member entities
- Texas Health Behavioral Health Virtual Visit
- Excludes the Texas Health joint venture entities (except those listed in the Formulation and Adoption of System-Wide Policies and Procedures in Section 4.1.6 or in Section 4.1.7)

1.2 Applicable Departments:
This policy applies to Texas Health's Workforce members, as well as members of Texas Health entity medical staff, trustees, contractors, and vendors who use Texas Health Workstations.

2.0 Purpose:

2.1 The purpose of this policy is to establish a standard for creation of strong Passwords, the protection of those Passwords, and the frequency of change.

3.0 Policy Statement(s):

3.1 All Texas Health employees (including contractors and vendors with Access to Texas Health Systems) are responsible for taking the appropriate steps to select and secure their Passwords.

3.2 References to third party sources and resources are intended for informational purposes only and not as procedural mandates.

4.0 Policy Guidance:

4.1 General Password Construction and Use

The section describes general Password construction for Users.

4.1.1 The length and complexity of Passwords shall always be checked automatically at the time that Users construct or select them.

a. For standard User accounts, all Passwords shall have at least eight (8) characters for all accounts.

b. For Privileged Accounts, all Passwords shall have at least twelve characters for all accounts.

4.1.2 All User-chosen Passwords shall contain at least a mix of upper-case and lower-case letters, a number (0-9) and at least one special character (!,@,#,$,%).

4.1.3 User chosen Passwords should not be any part of speech or common words found in a dictionary. For example, proper names, geographical locations, common acronyms, and slang should not be employed.

4.1.4 All User-chosen Passwords for computers and networks must be difficult to guess. Using derivatives of User-IDs, and common character sequences (such as "123456") should not be employed.

Adding numbers and special characters to dictionary words increases the complexity of the Password and the amount of time it takes an unauthorized individual, internal or external, to crack the Password. An example of a good Password is All?ergy2.

4.1.5 Personal details such as spouse's name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters.

4.1.6 Users shall not construct Passwords that are identical or substantially similar to Passwords they have previously employed.

4.1.7 Authorized Password strength tests may be performed on a periodic basis. If a Password is guessed or cracked during one of these scans, the User will be required to change it.

4.1.8 Passphrases are stronger than Passwords. A passphrase consists of the first letter of each word in a phrase. Including numbers and special characters, and mixing in upper and lower case characters further strengthens the passphrase. For example, I can't remember Passwords at 10 characters = Icrp@10c.

4.1.9 All standard Users are required to change their login Password at least once every one-hundred eighty (180) days, and every sixty (60) days for Privileged Accounts.

4.1.10 The previous twenty-four (24) passwords cannot be reused, and at least four (4) characters must be changed.

4.1.11 After ten (10) unsuccessful attempts to enter a Password, the involved User-ID should be either:

a. Suspended until reset by a System Administrator
b. Temporarily disabled for no less than fifteen minutes
c. Disconnected from any external network connections involved

4.1.12 Users shall not use their Texas Health Password for non-Texas Health Systems such as social media.

4.2 <u>Two Factor Authentication</u>

4.2.1 High risk authentication and access may be required to employ Two Factor authentication. Examples include:

a. ePrescribing Controlled Substances
b. Designated high risk remote access workflows
c. Designated privileged access accounts

4.2.2 All users assigned Two Factor authentication must be trained on how to use biometric or form factor technologies.

4.2.3 IT Risk Management and Assurance shall designate authorized Two Factor authentication issuing authorities. Issuing authorities verify the identity of the user and issue Two Factor capabilities such as tokens or biometric authentication.

4.2.4 IT Risk Management and Assurance shall approve Two Factor use cases and all Two Factor authentication enabling capabilities and form factors. This includes:

a. Biometric solutions
b. One-time password tokens
c. Smart cards

Users that are issued Two Factor tokens or smart cards shall ensure they are protected at all times. If a token or smartcard is lost or stolen users shall contact the ITS Service Desk as soon as possible.

4.3 <u>End USER Responsibilities</u>

4.3.1 Individual Users are granted responsibilities based upon the consent of least privilege.

4.3.2 Users are responsible for all activity performed with their personal User-ID's.

4.3.3 Passwords must not be written down, electronically stored, or left in a place where unauthorized persons might discover them.

If it becomes necessary to document a Password, Passwords shall be stored in CyberArk (Passwordvault).

4.3.4 Passwords must never be shared or revealed to anyone else besides the authorized User. If others need to share computer resident data, they should use electronic mail, public directories on local network servers, and other mechanisms.

4.3.5 All Passwords need to be promptly changed if they are suspected of being disclosed, or known to have been disclosed to unauthorized parties.

4.3.6 Users must not knowingly allow others to perform any activity with their uniquely assigned User-IDs. Similarly, Users are forbidden from performing any User activity with ID's belonging to other Users.

4.4 System Administrators

4.4.1 System Administrators are granted certain responsibilities related to Passwords.

4.4.2 There are cases where network computers, service accounts, Systems or Applications require a specific ID for maintenance responsibilities or System to System exchange of information. This Password must be documented and electronically stored in CyberArk.

4.4.3 The display and printing of Passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

4.4.4 All Privileged Accounts need to be automatically forced to change their login Password at least once every sixty (60) days.

4.4.5 System Administrators need to assign a unique Password for each User's first log-on session. At the initial logon time, the User is required to choose another Password before any other work can be done.

4.4.6 After ten (10) unsuccessful attempts to enter a Password, the involved User-ID should be either:

a. Suspended until reset by a System Administrator
b. Temporarily disabled for no less than fifteen minutes
c. Disconnected from any dial-up or other external network connections involved

4.4.7 Systems or Applications Administrators may disclose Passwords in a secure manner if:

a. A new User-ID is being assigned
b. The involved User has forgotten or misplaced the Password
c. The involved User is otherwise locked out of his or her User account

4.4.8 System or Application Administrators will not reveal a Password unless the involved User has first provided two pieces of definitive evidence substantiating his or her identity.

4.4.9 If a Password is sent by regular mail or similar physical distribution Systems, the Password must be sent separately from User-IDs. These mailings will have no markings indicating the nature of the enclosure.

4.4.10 If a Password is distributed by phone, the owner of the login is to be verified through two pieces of definitive evidence substantiating his or her identity.

4.4.11 No Password will be given to someone presenting the verification on behalf of another person.

4.4.12 If a Password is sent by email, the Password shall be separate from the login ID and the email shall be encrypted.

4.4.13 Passwords are never to be hard-coded (incorporated) into software developed by or modified by Texas Health workers.

4.4.14 All vendor-supplied default Passwords must be changed before the computer or communications System is deployed into the production environment.

4.4.15 Community strings, a type of Password, shall not be the default provided by the vendor.

4.4.16 Community strings will have a minimum number of eight (8) characters, for both read and write Access.

4.4.17 Community strings will have complexity where supported including alpha-numeric characters, uppercase and lower case, and special characters.

4.5 Application Development Standards

4.5.1 Application developers must ensure their programs contain the following security precautions:

a. Support authentication of individual Users
b. Does not store Passwords in clear text or in any easily reversible form
c. Provide for role-based Access management

4.6 Exceptions

4.6.1 Exceptions to this policy shall be processed through the policy exception process.

4.7 Policy Violations and Sanctions

4.7.1 Violations of this policy will be processed according to the applicable Texas Health policies, including the Progressive Corrective Action policy, as well as civil and criminal laws.

4.7.2 If you observe violations you must notify your supervisor, a representative of Human Resources, or the Compliance Hotline at 1-800-381-4728.

5.0 Definitions:

5.1 Access - The ability or means necessary to read, write, modify or communicate Data / Information or otherwise use any system resource.

5.2 Application - A set of files that makeup a software program designed for a specific use. These files have to be installed on a workstation or server. The set of files are generally composed of executables, configuration and ancillary data files. Examples of Applications are Microsoft Exchange, Epic and Internet Explorer

5.3 Application Administrator - The person who is responsible for administering the Application, and maintenance activities which could include assigning Access.

5.4 Encryption - A method used to convert Data from a readable clear text format to an unreadable format. This method is achieved by using an encryption algorithm that combines plaintext with other values called keys, or ciphers, so the data becomes unintelligible.

5.5 Password - A password is a sequence of characters used to verify that a computer User requesting access to a computer system is really that particular User.

5.6 Privileged Account - An account that has elevated Access to perform additional activities. For example, this may be an account with local administrative access, or an account beginning with the character "~". This character signifies different access.

5.7 System - A group of related components (e.g. central processing unit (CPU), operating system and peripheral devices) that interact to perform a specific task. Examples of systems are workstations, servers, and mainframes.

5.8 System Administrator - The person who is responsible for administering the platform, including the operating System, and maintenance activities which could include assigning Access.

5.9 Trustee/Director - Refers to a person who serves as a member of the governing board of Texas Health or any of its wholly owned or wholly controlled corporations pursuant to the bylaws of the respective corporation.

5.10 Two Factor - Authentication that requires two forms of authentication. Also known as strong authentication. The two forms are selected from three choices: Something you know (password), Something you are (biometric) or something you have (token).

5.11 Users - Texas Health Workforce members, members of Texas Health facility Medical Staff, Trustees/Directors, contractors, vendors, or others who use the Texas Health Electronic Communication Systems.

5.12 User ID - A combination of characters sometimes based upon letters taken from the last and first names of a user, representing who the user is, and is used to log into a system.

5.13 Workforce - Employees, volunteers, persons involved in Texas Health training programs, or those sponsored by its wholly owned or wholly controlled entities, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether or not they are paid by the entity.

6.0 Responsible Parties:

6.1 IT Risk Management & Assurance

6.1.1 Manages and participates in the development of Information Security policies and standards; identifies security risks; performs risk-based assessments to ensure that Information Security risks are maintained at levels that are acceptable to Texas Health management.

6.2 Service Desk

6.2.1 Responsible for first level support in conducting routine tasks (i.e. password creation, resets, two-factor token administration).

6.3 Texas Health Workforce, Trustee and Medical Staff

6.3.1 Responsible for complying with the Password Management policy, and for managing and maintaining secure Passwords for the purpose of protecting Texas Health information.

6.4 System Owner

6.4.1 Participates in the development and maintenance of IT policies and standards. Responsible for purchase, support, maintenance and security of assigned Systems.

7.0 External References:

7.1 CMS.GOV. (n.d.). CMS.gov Home Page. Retrieved from https://www.cms.gov/.

7.2 Health Information Trust Alliance (HITRUST). (n.d.). Retrieved from https://hitrustalliance.net/.

7.3 HHS.gov (2013, July 26). Summary of the HIPAA Security Rule, 45 CFR § 160.103 and Subparts A and C…[19] 45 CFR § 164..308(a)(1)(ii)(C), from http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

7.4 NIST.gov. NIST 800-30, 800-52, 800-66, 800-77, 800-88, 800-111, 800-113. http://nist.gov/.

7.5 NIST.gov. (2001, November 15). FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Retrieved from http://csrc.nist.gov/groups/STM/cmvp/standards.html.

7.6 OWASP.org. (2001, December 1). Open Web Application Security Project (OWASP). Retrieved February 15, 2016, from https://www.owasp.org/index.php/Main_Page.

8.0 Related Documentation and/or Attachments:

8.1 Data Access Control Policy

8.2 Electronic Communications Acceptable Use Policy

8.3 Information Privacy and Security Sanctions Policy

8.4 Minimum Necessary Use and Disclosure of Health Information Policy

8.5 Progressive Correction Action Policy

9.0 Required Statements:

Not Applicable