THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: IT0506-HSC-A.01 Password Management and Complexity	
Version 8	Effective Date: 03/17/2016

Responsible Office: Office of Cybersecurity	Last Review: 03/01/2025 Next Review: 03/01/2027
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

Users of the University of Tennessee Health Science Center (UTHSC) networks, systems, or applications are supplied with a unique user account ID and a password, (i.e. a password, pass-phrase, or PIN), or other individually identifiable authentication method, to gain access to such systems and to protect them from unauthorized use. A poorly chosen password, passphrase, or PIN may result in unauthorized access and/or exploitation of UTHSC data and systems. This practice guides users in creating, protecting, and changing passwords so they are strong, secure, and protected.

Scope

This practice applies to all members of the UTHSC community, representing UTHSC in any capacity, who have been granted access to any system or data by means of an authenticator, based on a unique user account ID and password. (i.e. a password, PIN, passphrase, etc.)

Definitions

Multifactor authentication: a method of computer access control that requires the user to provide two or more verification factors to gain access to a UTHSC resource.

Passphrase – a memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage but is generally longer for added security.

Password - a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

PIN – Personalized Identification Number – a memorized secret typically consisting of only decimal digits.

Responsibilities

UTHSC Campus Community is responsible for creating strong passwords or passphrases and keeping those protected, ensuring the security of the campus.

THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER.

Practice

1. All users with access to any systems, networks, and/or data while representing UTHSC are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.
2. Any user suspecting that their password may have been compromised must report the incident to the Office of Cybersecurity and change all affected passwords.
3. Any suspected or known compromised accounts will be investigated by the Security Incident Response Team in accordance with IT0017-HSC-A Security Incident Response.
4. Shared accounts and passwords shall not be used except in the following situations:
   a. When multiple administrative system accounts cannot be established. In such case, a risk assessment should be performed by the system owner. Mitigation of the assessment would include documented procedures to safeguard the account credentials.
   b. Multi-use workstations may have a generic account for access to the device only, in which case no data or information classified other than Public may be stored on the device.
5. Passwords must meet the following requirements:
   a. General
      i. Default passwords included as part of any system must be changed as soon as practical with a password that complies with the Complexity Requirements (5.b below), and in all cases prior to the system being placed onto any network. This includes, but is not limited to, SNMP community strings.
      ii. Passwords stored in clear-text in any form (including paper) or format must be kept either in a secured system or encrypted.
      iii. Transmission of passwords by any means must use encryption. When communicated orally, precautions must be taken to prevent password from being overheard by unauthorized individuals.
      iv. The passwords to system and service accounts essential to the operation of an information system must be known or accessible to more than a single person. Such passwords must meet the

complexity requirements, be stored in a secure manner, and changed on a schedule relative to the risk of exposure and at a minimum when those with knowledge of the password terminate or are re-assigned.

 v. Upon creation or reset of an account, the system should prompt the user to create an initial password that complies with the Complexity Requirements (5.b below). In cases where this is not possible, the initial password must be unique, comply with the Complexity Requirements, and require that the user change the password upon the first use.

 vi. Passwords should be unique for each account or access point. Do not reuse the same passwords for multiple accounts.

 vii.

b. Complexity Requirements

 i. Be a minimum length of 16 characters and no more than 40 characters in length

 ii. Contain some combination of at least three of the following:
- Uppercase letters
- Lowercase letters
- Numbers
- Punctuation & Symbols (Accepted: `` `!@#$^&*()_-={}|[]:;'<>?, ``)

 iii. May not contain a significant portion of your username or displayname

 iv. Not be a word in any dictionary

 v. Not be solely based on easily guessed personal information, names of family members, pets, etc.

c. Reuse

 i. Not allowed to reuse last 10 passwords

d. Special requirements

 i. Multifactor authentication is required for all privileged accounts on all university systems, whether managed on-site or vendor hosted.

e. Change Timeline

 i. Passwords must be changed every 180 days for accounts that do not use multifactor authentication.

 ii. Passwords must be changed immediately for a known or potential

account compromise.

Policy History

Version #	Effective Date
1	03/17/2016
6	10/02/2020
7	01/12/2023
8	03/01/2025

References

1. IT0506-Information Technology Account and Credential Management
2. IT0017-HSC-A-Security Incident Response
3. IT0311-HSC-A-Access Control
4. IT0506-HSC-A-Authentication
5. NIST Glossary of Terms