THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: AC-002-Authentication	
Version 6	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 11/17/2020 Next Review: 11/17/2022
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

Authentication mechanisms such as username and passwords combinations are the primary means of obtaining access to computer systems and data. It is essential that these authenticators be strongly constructed and used in a manner that prevents their compromise. They are designed to minimize the potential security exposure to UTHSC from damages which may result from unauthorized use of UTHSC resources. Multi-factor authentication is an additional protection to systems and applications.

Scope

This standard applies to members of the UTHSC Community who have been granted access to UTHSC IT Resources and/or represent UTHSC in any capacity.

Definitions

Central Authentication Service (CAS): is a sign-on protocol that authenticates users to multiple systems using the same authenticators, i.e. NetID and password.
DUO: UTHSC's multi-factor authentication application
Multi-factor 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.
UTHSC Resource: Any data, device, or other component of the information environment that supports information-related activities. Assets generally include hardware (e.g. endpoint devices), software (e.g. critical applications and support systems), and information.

Responsibilities

Office of Cybersecurity is responsible for setting basic security standards for the UTHSC Resource.
ITS Infrastructure team is responsible for the deployment of technical controls to establish authentication.
UTHSC Community is responsible for adhering to this standard and the security controls set forth in it to prevent unauthorized access using their authenticators or credentials.

Standard

1. Access to all university data and systems not intended for unrestricted public access requires authentication.
2. All users of networks, systems, or applications must be supplied with a unique authenticator, i.e. UTHSC NetID and a password, or other individually identifiable authentication method, to gain access to such systems to protect from unauthorized use.
3. The individual registered as the owner of the authenticator accessing UTHSC data, information, and systems is responsible and liable for all processes initiated with that authenticator. Unacceptable use, whether intentional or unintentional, will result in immediate suspension of the access privileges.
4. Authenticators must be constructed in compliance with the complexity standard for the employed authenticator, for example, passwords must comply with Practice-InfoSec-AC-002.02 Password Management and Complexity.
5. Users are required to use multi-factor authentication (MFA) in accessing UTHSC systems and applications.
    a. Users will be required to enroll a device to serve as the second authentication method as part of MFA. This device may be a cell phone or DUO token.
    b. Information about UTHSC's MFA solution, DUO, can be found on this webpage.
6. No one may share or require another to share authenticators to individually assigned access to any systems or data while acting as a

representative of UTHSC.

7. Generic or group authenticators are not permitted except for business justified requested exemptions and exceptions, if sufficient other controls on access are in place.
8. UTHSC applications and systems are designed to authenticate using Central Authentication Service (CAS) using UTHSC NetID and password along with DUO MFA.
9. Applications and systems that do not have users authenticate using NetIDs must establish an alternative mean of authentication, using MGA if such authentication is supported.
10. UTHSC systems must be designed and configured to protect authentication factors during storage and transmission utilizing the data ranking system designed in Standard-InfoSec-GP-002-Data & System Classification.
11. Any, either known or suspected, compromise of an authenticator must be immediately reported to the access grantor and the authenticator changed.
12. Suspected or known compromises should be reported to, and investigated by, the by Security Incident Response Team in accordance with Standard-InfoSec-IR-001-Secuity Incident Response.
13. Exceptions to this Standard should be requested using the process outlined in Practice-InfoSec-GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices.

References

1. Standard-InfoSec-AC-001-Access Controls
2. Standard-InfoSec-GP-002-Data & System Classification
3. Practice-InfoSec-AC-002.02 Password Management and Complexity
4. Standard-InfoSec-IR-001-Security Incident Response
5. Practice-InfoSec-GP-001.02 Security Exceptions and Exemptions to ITS Standards and Practices