THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: IT0506-HSC-A Authentication	
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

Authentication mechanisms such as username and password combinations are the primary means of accessing computer systems and data. These authenticators must be strongly constructed and used in a manner that prevents their compromise. They are designed to minimize the potential security exposure to the University of Tennessee Health Science Center (UTHSC) from damages resulting from unauthorized use of UTHSC resources. Multifactor 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 multifactor authentication application
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.
UTHSC Information Technology (IT) Resource - a broad term for all things related to information technology from a holistic point of view and covers all University-owned or managed information technology services, including cloud-based services, that users have access to.

Responsibilities

Office of Cybersecurity is responsible for setting basic security standards for the UTHSC Resource.
ITS Infrastructure team is responsible for deploying technical controls to establish authentication.
UTHSC Community is responsible for adhering to this standard and the security controls outlined 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 IT0506-HSC-A.01-Password Management and Complexity.
5. Users must use multifactor authentication (MFA) when 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 means of authentication, using MFA 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 IT0005-HSC-A-Data & System Categorization.

11. Any compromise of an authenticator, either known or suspected, 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 IT0017-HSC-A-Secuity Incident Response.
13. Exceptions to this Standard should be requested using the process outlined in IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards, Practices, and Controls.

Policy History

Version #	Effective Date
1	03/17/2016
4	06/17/2020
5	11/19/2021
6	05/12/2022
7	02/15/2023
8	03/01/2025

References

1. IT0506-Information Technology Account and Credential Management
2. IT0003-HSC-A.02-Security Exceptions and Exemptions to ITS Standards, Practices, and Controls
3. IT0005-HSC-A-Data & System Categorization
4. IT0017-HSC-A-Security Incident Response
5. IT0311-HSC-A-Access Controls
6. IT0506-HSC-A.01-Password Management and Complexity