THE UNIVERSITY OF TENNESSEE
MARTIN

UT - Martin Policy: IT0132-M - Identification and Authentication Program	
Version: 5	Effective Date: 08/01/2023

Objectives:

To establish formal, documented identification and authentication program for managing risk from user access and authentication into critical information systems.

Scope:

This program applies to all users of, and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Martin (UTM) including its regional centers.

"Users" includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this program is based on those guidelines. This plan is based on guidelines in *NIST SP 800-53 Revision 5.1, Recommended Security Controls for Information Systems and Organizations*.

UTM must develop or adopt and adhere to a program that demonstrates compliance with related policies and standards. This program is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of University policy is assumed if a User accesses, uses, or handles University resources.

UT - Martin Policy: IT0132-M - Identification and Authentication Program	
Version: 5	Effective Date: 08/01/2023

Program Details:

This program establishes the implementation of select controls used in identifying and authenticating users and systems before allowing access to information, applications, or systems. This program is to be reviewed annually (IA-1).

Roles and Responsibilities:

Chief Information Officer: Has overall accountability of this Identification and Authentication Program as the Position of Authority.

Director of IT Security: Responsible for overseeing the implementation, monitoring, and maintenance of this program.

Account Management (AC-2):

Accounts are managed using Active Directory (AD) where technically feasible. Information system account usage is monitored to help protect against misuse and detect compromised accounts.

Access Enforcement (AC-3):

The information system enforces approved authorizations for logical access to information and system resources.

Identifier Management (IA-4):

New employees are entered into the IRIS system. UTM receives a file with the employee's information from IRIS and creates an AD account in the UTM forest.

Temporary/guest accounts can be created by employees for use by individuals not affiliated with UTM or the University. The maximum lifetime for a given temporary account is five (5) days. The page for creating temporary accounts is https://utm.teamdynamix.com/TDClient/2421/ITS-Portal/Requests/ServiceDet?ID=47163

Disabled Faculty, Staff, and Sponsored accounts will be deleted 1 year after being disabled.

Authenticator Management (IA-5):

When a new employee AD account has been created, the password is set to the default. The default password is formatted **Mon#YYYY#SSSS**

Mon is the first 3 letters of birth month, with the first letter capitalized,
YYYY is four-digit birth year,
SSSS is the last 4 digits of Social Security Number

Authenticator Feedback (IA-6):

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

Additional Information:

More information on password requirements, account inactivity, and service account requirements can be found in *IT1002-M - Password Standard.*

Banner Administrative Access

See *IT0132-M-A - Banner Administrative Access Request Overview* for more information regarding this process.

UT - Martin Policy: IT0132-M - Identification and Authentication Program	
Version: 5	Effective Date: 08/01/2023

References:

IT0132 - Identification and Authentication

IT0132-M-A - Banner Administrative Access Request Overview

IT1002-M - Password Standard

NIST SP 800-53 Revision 5.1, Recommended Security Controls for Information Systems and Organizations

Definitions:

Account Management: The identification of authorized users of the information system and the specification of access privileges.

Active Directory (AD): The Windows OS directory service that facilitates working with interconnected, complex, and different network resources in a unified manner.

Authenticator: The means used to confirm the identity of a user, process, or device (e.g., user password or token).

Forest: The topmost logical container in an AD configuration that contains domains, users, computers, and group policies; the security and administrative boundary for objects and entities.

Identifier: Unique data used to represent a person's identity and associated attributes.