UTC-S-IT0132 – UTC Identification and Authentication Standard

Objective:
To align University of Tennessee at Chattanooga (UTC) standards of practice with University of Tennessee System-wide policy for developing, maintaining and documenting an Identification & Authentication program.

Scope:
This program applies but is not limited to employees, contractors, agents, and representatives accessing, using, or handling UTC information technology resources.

Principles:
This document is a UTC-specific Standard based on University System-wide policy. Each User of UTC resources is required to be familiar and comply with University policies, and acceptance is assumed if the User accesses, uses, or handles UTC information technology resources.

The Chief Information Officer (CIO) is the Position of Authority (POA) for Information Technology at UTC and responsible for IT security at the University of Tennessee Chattanooga.

Responsibilities:

1. The CIO has overall responsibility of the Identification & Authentication (IA) program at UTC and ensures:
    a. The program is developed, documented, and disseminated to appropriate UTC entities in accordance with University policy.
    b. The program is reviewed and updated annually.
2. The Chief Information Security Officer (CISO) is responsible for overseeing the Identification & Authentication program and consulting system owners to ensure effective procedures are implemented.
3. System owners/administrators are responsible for adhering to this Standard for their respective system(s).

Standard:

1. All business systems supporting mission-essential functions are included in UTC's Identification & Authentication program.
2. System owners and administrators must develop, document and maintain Identification and Authentication processes and procedures that address:
    a. Unique User ID's (e.g. via UTC Net ID abc123) and passwords.
    b. Use of strong passwords.
    c. Reporting lost or compromised user accounts or passwords.
    d. Revoking passwords when they are lost or compromised.
    e. Defining a period of inactivity, after which a User ID is disabled.
    f. Establishing management guidance for shared information system accounts (e.g. service, guest, and anonymous accounts).
    g. Changing default authenticators upon information system installation;

h. Changing/refreshing passwords periodically as appropriate.
i. Critical information systems must mask passwords during the authentication process to protect the information from possible unauthorized use.

3. Password Enforcement (effective July 1, 2017)
    a. Passwords will expire and must be reset (once every 180 days for regular employees; 60 days for IRIS users)
    b. Upon expiration, accounts will be locked until the password is reset.
    c. Go to https://ds.utk.edu/passwords to change your password.
    d. Password history will be enforced. Choose a new password every time it is reset.
    e. Passwords must meet the following minimum complexity requirements:
        i. Be a minimum of 8 and no more than 16 characters in length
        ii. Contain some combination of at least three of the following:
            1. Uppercase letters
            2. Lowercase letters
            3. Numbers
            4. Punctuation & Symbols
            5. (Accepted: `~!@#$^&*()_-={}|[]:;'<>?,)
        iii. May not contain a significant portion of your username or display name.
        iv. May not reuse last 10 passwords.
    f. Password tips:
        i. At UTC we highly recommend using a "passphrase" variant that you can easily remember. For example, "I'm graduating!" could become your passphrase "I'mgr@du@ting!"
        ii. Use a different password for your NetID from your personal online accounts, such as Twitter, Instagram, and Facebook.
        iii. Do not use your UT NetID or UT email address as the username for your personal accounts.
        iv. Do not write your password down.
        v. Never use the names of your family, pets or favorite sports teams as your password.
        vi. Never use dictionary words in any language as your password unless you are using a passphrase.
        vii. Consider using a password vault such as LastPass or KeePass.

References:

UT Policy IT0132 – Identification and Authentication