Password Policy

Document Number: ITS-0015 **Date Published(sys):** 11/15/2021

General Description

Purpose:

Trinity University is committed to a secure information technology environment in support of its mission[1]. In today's constantly changing cyber threat landscape, the need for a strong password policy is greater than ever. Many systems at the University require the use of passwords including but not limited to e-mail, academic and administrative applications, computing labs, and VPN. Strong passwords result in strengthening the security of Trinity University's entire network and a consistent measure of protecting the University's Information and Technology resources as well as the safeguarding of personal and confidential information of the University community.

Within this Policy, the terms "Trinity University", and "Trinity" may be used interchangeably.

Scope:

The Password Policy applies to all persons accessing the Trinity University's Network, systems, and applications (hereafter referred as "users"), include students, faculty, staff, third party contractors, visitors (guests), consultants and employees fulfilling temporary or part-time roles.

The Password Policy serves as a minimum requirement for configuration of passwords on Trinity applications and systems. Trinity applications and systems must be configured to conform as closely as possible to these requirements within the Trinity systems or application's capabilities. For those systems or applications that do not have the capability of enforcing the security controls mentioned in this policy, an exception must be documented with written permission from the CIO.

Policy Content

1 1.0 Policy

- 1.1 Password Construction Standard

Password mechanisms are used to access various Trinity systems, including Trinity's network, e-mail, and various Trinity applications. Below best practices must be followed for password configuration on Trinity systems for end-user account passwords, admin account passwords, and system service account passwords.

1. Passwords must be 12 characters long minimum, and a maximum length of 64 characters.
2. Passwords must contain, at minimum:
    - 2 or more uppercase characters (A through Z)
    - 2 or more lowercase characters (a through z)
    - 2 or more numerals (0 through 9)
    - Optional Non-alphabetic characters (for example . , !, $, #, %)
3. Passwords must be changed every one hundred eighty (180) days.
4. At a minimum, twelve (12) previous passwords must not be repeated for a particular Trinity system or application.
5. Users will be notified at least fourteen (14) days in advance of password expiration on each Trinity system or application. Upon receiving the password expiration notification, Users must be prompted to change their password.
6. Passwords must not contain the user's account name or parts of the user's full name which exceed four (4) consecutive characters of the user's name.

- 1.2 Password Protection Standard for Users

1. Passwords must be treated as confidential information. A user must not disclose or hint at their password to another person, including Trinity IT staff, administrators, superiors, other co-workers, other users, friends, and family members, under any circumstances.
2. Passwords must not be transmitted electronically over the unprotected Internet without encryption or other protections.
3. A user must not keep a written record of their passwords, either on paper or in an electronic file.
4. A user must not use dictionary words while constructing passwords.
5. A user must avoid repetitive or sequential characters (example: 'aaaaaa', '1234abcd').
6. A user must not use context-specific words, such as the name of the service, the username, and derivatives thereof.
7. Passwords used to gain access to Trinity systems or applications must not be used as passwords to access non-Trinity systems or applications.
8. If a user either knows or suspects that one of their passwords have been compromised, the User must change the password immediately and notify the Trinity IT Department.

Performance Evaluation

Consequences of Policy Violation:

Any behavior in violation of this policy is cause for disciplinary action and violations of this policy may result in, but are not limited to, any or all of the following:

- Loss of university computing, email and/or voice mail privileges
- Disconnection from the residential hall internet network
- University judicial sanctions as prescribed by the student code of conduct
- Monetary reimbursement to the university or other appropriate sources
- Reassignment or removal from university housing and/or suspension or expulsion from the university
- Prosecution under applicable civil or criminal laws

Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources.
Reports of compromised passwords should be reported to ITS immediately:

- Email: itsupport@trinity.edu
- Phone Number: 210.999.7409

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.
Identity	An attribute or set of attributes that uniquely describe a subject (A person, organization, device, hardware, network, software, or service) within a given context.

Related Documents

Related Content:

This Trinity University Password Policy is aligned with NIST Special Publication 800-63B, a standardized security framework for Digital Identity Guidelines for Authentication and Lifecycle Management. In addition, this policy is aligned with applicable laws and regulations including HIPAA and FERPA.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v3.0	11/15/2021 2:49 PM	Ben Lim
v2.0	9/29/2021 1:58 PM	Dan Carson
v1.0	8/14/2019 5:06 PM	Courtney Cunningham

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer