

Password Policy

Overview

Passwords are an important aspect of computer security at the University of St. Thomas. They are the first line of defense for the user accounts and network infrastructure. A poorly chosen password could result in the compromise of critical University systems and potentially the entire network. As such, all users of University technology resources are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish the requirements for appropriate security for UST accounts. These requirements are necessary to help ensure personal security and protection of University business and academic data.

Scope

The scope of this policy includes all **users** who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any University facility, has access to the University network, or stores any non-public University information.

Passwords

Passwords may be used only by the authorized user. Passwords or accounts should never be shared with anyone, including trusted friends or family members. Account owners will be held responsible for any actions performed using their account UST IT staff will **never** ask users to disclose their passwords in any manner.

Passwords for University technology resources must comply with the following standards:

- All passwords (e.g., email, myStThom, Blackboard, desktop computer, etc.) must be changed every 120 days.
- All passwords must be at least 8 characters in length.
- All passwords must contain at least one number (0-9) or special character* (~, !, @, #, \$, %, ^, &, *, (,), -, =, +, ?, [,], {, }).
- All passwords must differ from a person's username.
- All passwords must contain at least one upper case letter (A-Z).
- All passwords must contain at least one lower case letter (a-z).
- **Password History:** systems should be configured to require a password that is different from the last five (5) passwords.

**Be aware that some university systems may not support non-alphanumeric characters or only support a specific subset.*

Violations

Violation of this policy will subject users to existing University disciplinary procedures and may result in loss of technology privileges. Illegal acts involving University technology resources may also subject violators to prosecution by local, state, and/or federal authorities.