Springfield Technical Community College

Password Policy

POLICY
Password Policy

POLICY CATEGORY
Information Technology Services

PURPOSE
The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the necessity to routinely change those passwords that are used to connect to Springfield Technical Community College (STCC) information technology resources. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

SCOPE
This policy applies to any person utilizing STCC information technology resources. The following persons ("users") are authorized to use STCC information technology resources: (1) current faculty; (2) current staff; (3) current students; (4) authorized contractors or vendors; and (5) authorized visitors.

POLICY
Passwords are an important safeguard of information security. A poorly chosen password may result in unauthorized access and/or exploitation of college resources, including personal identifiable information (PII). All users with access to college systems are responsible for taking the appropriate steps to select and secure their passwords as outlined below.

- All user-level and system-level passwords must conform to the password security procedures defined by Information Technology Services, including:
  - Passwords must be changed according to the password reset interval,
  - Minimum password requirements must be met according to password complexity rules,
  - Password history is set to 10, which is the number of unique passwords that must be set before an old password can be reused,
  - Passwords are locked after (4) unsuccessful attempts.
- Each user is responsible for maintaining the confidentiality of passwords that are used to gain access to STCC systems and services.
- Passwords should not be shared with anyone. All passwords are to be treated as sensitive and confidential information.
- Passwords should not be written down or stored/transmitted electronically without the use of encryption.

- Users should never attempt discovery of a system or another user's passwords, either manually or utilizing an automatic password cracking system.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges.
- Any user suspecting that his/her password may have been compromised must report the incident to Information Technology Department and change all passwords immediately.

MULTI-FACTOR AUTHENTICATION

Beginning on April 3, 2023, all STCC faculty, staff, vendor, and other accounts provisioned in the stcc.edu domain will be required to use DUO Multi-Factor authentication (MFA) to access the Virtual Private Network (VPN) and Google Workspace applications. This requirement is subject to change and other systems may be included in MFA based on the requirements set by the College's cyber security insurance provider.

ENFORCEMENT

Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights, expulsion from the college or termination of employment. Depending upon the nature of the violation of this policy, a user may also be subject to civil liability and/or criminal prosecution.

REVISION HISTORY

This section contains information on the approval and revision history for this policy.

Version Number	Issued Date	Approval	Description of Changes
1.0	3/2016	Massachusetts CIO Council	Development and adoption of collaborative and standardized IT policies
1.0	7/2016	Massachusetts Community College Counsel's Office	Recommendation on contents provided by college counsel
2.0	8/2021	Trustee Internal/External Committee	Policy revision and review
2.0	8/2021	College Adoption	Revisions implemented
3.0	12/2022		Addition of Multi-Factor Authentication and Password rules