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

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.