Springfield Technical CommuWB

systems (with auto-update enabled), web browsers, and common applications shall be applied. A firewall must be enabled on each applicable device.

- Remote access services may be used only to conduct business-related work. Personal, private, or commercial use of any service available remotely is not permitted.

- Users agree to protect STCC information assets from unauthorized access, viewing, disclosure, alteration, loss, damage, or destruction.

- Remote access to data or services may not be used to copy private or personal information such as that residing on a privately owned computer, to company file shares, or other company-owned information systems.

- Remote access to data or services may not be used to store College information on a personal system, file share or other non-College owned system without prior, written approval from the AVP/Chief Information Officer.

- Some systems may require Multi-Factor Authentication (MFA) for enhanced security. IT reserved the right to implement MFA as necessary.

ENFORCEMENT

Any employee found to have violated, intentionally or unintentionally, this policy may be subject to disciplinary action, up to and including termination of employment.

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	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