



Springfield Technical Community College Remote Access Policy

PURPOSE

The purpose of this policy is to define the process and requirements for connecting to the Springfield Technical Community College (STCC) network from any remote system. These requirements are designed to minimize potential damages to the STCC network, which may result from such remote access and/or unauthorized use of College resources. Damages include, but are not limited to the breach of confidential, sensitive, or organizational information and intellectual property, damage to public image, damage to critical internal systems, the compromise of system functionality, or the corruption of information integrity.

This policy must be read in conjunction with the **Acceptable Use of Information Technology Resources Policy**.

SCOPE

This policy applies to all STCC employees, students, contractors, and third parties who may access STCC applications, systems, or hardware remotely. This policy does not apply to external (public) facing systems designed to be used via the web.

POLICY

All remote access to STCC applications, systems and hardware shall be authorized and approved in advance, and any access not explicitly authorized and approved is prohibited. Remote access to specific applications, systems, components and technology infrastructure shall only be granted to users with a legitimate business or academic need for such access. The level of access granted and privileges assigned shall be limited to the minimum required to perform assigned duties.

- Employees and third parties authorized to utilize remote connections shall ensure that unauthorized users are not allowed access to the STCC internal network utilizing these connections.
- All individuals and devices, including college owned and personal equipment, are an extension of STCC's network. All STCC issued laptops will be set up with the VPN software after approval from the division Vice President and the AVP/Chief Information Officer. Access will be granted to allow users to access authorized systems and services remotely. All users will be responsible to follow this policy and procedures to protect STCC data and property.
- Users are prohibited from downloading, installing, or using any VPN software on personal devices to access the STCC network.
- All devices, including personally-owned computers that are connected to the network via remote access technologies must use the most updated version of anti-virus software and available patches. Security patches for installed operating

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 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