OFFICE OF INFORMATION TECHNOLOGY
REMOTE ACCESS

I. PURPOSE AND SCOPE

This rule helps protect college IT resources, Information Systems, and Information Assets when accessed remotely. This Rule applies to remote access connections used to perform work for or on behalf of SLCC. This Rule supports Procedures section J, titled Remote Access, of SLCC Information Security Policy.

II. DEFINITIONS

A. **Authentication Credentials (credentials):** user identification (ID) and personal identification number (PIN), username and password, or other secrets or keys used to gain access to a restricted resource.

B. **Remote Access:** access to information assets from any location outside of the college's network or physical boundaries.

C. **User (Authorized User):** any person, including students, staff, faculty, permanent and temporary employees, contractors, vendors, research collaborators, and third-party agents, who accesses any college electronic resources, information systems, or IT resources.

D. **VPN**: a virtual private network that uses a public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to the college's network.

III. PROCEDURES

A. Remote User Access Methods

All remote access methods are covered by this rule, including but are not limited to Citrix, Remote Desktop Protocol (RDP), Secure Shell (SSH), and VPN.

B. Remote Access Requirements

Prior to issuing access to the college's remote access technologies, OIT controls remote access requires the use of unique user authentication credentials and authentication.