Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Remote Desktop/Virtual Private Network Access Policy:

PURPOSE:
The Remote Desktop/Virtual Private Network Access Policy exists to protect Clarendon College's information technology resources. Restricting remote access partly ensures the security of the information technology resources in the Clarendon College domain. Remote Desktop (RDP) or Virtual Private Network (VPN) allows Clarendon College users (Regular and Visitor Account users as defined in Policy) to securely access the university's network via an existing connection to the Internet from a remote location.

RDP or VPN connections present an increased security risk if the connecting computer is insecure. Security, Internet access, and configuration of the connecting computer are solely the responsibilities of the user account holder making the connection.

SCOPE:
The Clarendon College Remote Desktop/Virtual Private Network Access policy applies equally to all individuals with authorized RDP or VPN accounts accessing Clarendon College information technology resources.

POLICY STATEMENT:
1. individuals with RDP and/or VPN privileges are responsible for ensuring that unauthorized users are not allowed access to the Clarendon College network using their security credentials.

2. RDP/VPN authentication is controlled using Clarendon College user account credentials.

3. Clarendon College-IT manages RDP/VPN gateways.

4. All computers connected to the Clarendon College network via RDP/VPN or any other technology must use the most up-to-date anti-virus software, regardless of the type or ownership of the device.

5. RDP/VPN users will be automatically disconnected from Clarendon College's network after a designated time-out period determined by Clarendon College-IT. The user must then log in again to reconnect to the network.

6. Pings or other network utilities must not be used to keep the RDP/VPN connection open.

7. Non-Clarendon College-owned equipment must be configured in compliance with Clarendon College policies and procedures.

8. Using RDP/VPN technology with personal equipment, users must understand that their machines are a de facto extension of Clarendon College's network. RDP/VPN users and privately owned equipment must comply with Clarendon College policies and procedures (See Personally-Owned Device Usage Policy).

9. RDP/VPN access does not guarantee access to all campus systems/applications. Access to systems/applications will be evaluated on a case-by-case basis.

DEFINITIONS:
Unauthorized user: A person without official permission or approval to access Clarendon College systems.

Virtual Private Network (VPN): Extends a private network across a public network, like the internet, to provide remote offices or individuals with secure access to the Clarendon College network using special hardware and software.

Remote Desktop (RDP): A program or an operating system feature that allows a user to connect to a computer in another location, see that computer's desktop, and interact with it as if it were local

A VPN Gateway (Also known as a VPN Router) is a connection point connecting two networks connected by a non-secure network such as the Internet.

Related Policies, References and Attachments:
An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.