CLARK UNIVERSITY

Clark University's Remote Access Policy

What is the purpose of this policy?

The purpose of this policy is to state the requirements for remote access to computing resources hosted at Clark University using Virtual Private Network (VPN) technology.

What is a Virtual Private Network (VPN)?

In order to access computing resources hosted at Clark University from off-campus, use of our Virtual Private Network is required. A Virtual Private Network (VPN) is a secured private network connection built on top of a public network, such as the Internet. A VPN provides a secure encrypted connection or tunnel over the Internet between an individual computer (such as a computer off campus) and a private network (such as Clarks). Use of a VPN allows members of the Clark University community to securely access Clark University network resources as if they were on the campus.

- **Get Connected with the VPN**
  Get more information about how to use the VPN and login with your Clark credentials to download the directions and installer files.

Who can use the VPN?

All Clark University students, employees, and authorized third parties (customers, vendors, etc.) may utilize the benefits of the VPN to access Clark University computing resources to which they have been granted access. In order to use the VPN, you need a connection to the Internet from your off-campus location. Clark does not provide you with an Internet connection, your Internet Service Provider does. While dialup Internet connections can utilize a VPN connection, performance is very slow and is not recommended or supported.

What are the "terms of use" associated with remotely connecting to Clark resources and using VPN?

1. It is the responsibility of all Clark University employees, students, and authorized third parties with VPN privileges to ensure that unauthorized users are not allowed access to internal University networks and associated content.
2. All individuals and machines, while using Clark's VPN technology, including university-owned and personal equipment, are a de facto extension of Clark University's network, and as such are subject to the University's Acceptable Use Policy.
3. All computers connected to Clark University's internal network via the VPN or any other technology must use a properly configured up-to-date operating system and anti-virus software; this includes all personally-owned computers. Antivirus software is available for faculty, staff and students of Clark University.
4. Redistribution of the Clark University VPN Installer or associated installation information is prohibited.

5. All network activity during a VPN session is subject to Clark University policies.
6. All users of the Clark VPN shall only connect to or have access to machines and resources that they have permission and rights to use.

What else should I know about Clark's University's VPN service?

1. The Information Technology Services department has created a VPN installer to assist Windows users with access to the VPN. Clark Universitys VPN installer requires the use of Internet Protocol Security (IPSec). The installer will make sure the IPSec service on your local computer is started and set it to automatically start every time the local machine is restarted.
2. When actively connected to the university network via the VPN, all network traffic destined for Clark University's network will travel across the VPN tunnel. All other traffic will go through the user's Internet Service Provider (ISP).
3. VPN users will be automatically disconnected from the Clark University network after 30 minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes to keep the connection open are prohibited.
4. Support will only be provided for VPN clients approved by Clark University's Information Technology Services.
5. If you have any questions related to the use of the Clark University VPN, please contact the ITS Help Desk (508-793-7745).

What happens if the "terms of use" are violated?

Any user found to have violated the terms of use may be subject to loss of privileges or services and other disciplinary action.

Who do I contact in the event of a remote access or VPN policy dispute?

The Chief Information Officer is charged with the responsibility to periodically review the policy and propose changes as needed.

Date of Creation: November 19, 2007
Date of Last update: February 26, 2007