Policy Name: Remote Network Access
Originating/Responsible Department: Information Technology Services (ITS)
Approval Authority: Senior Management Committee
Date of Original Policy: February 2010
Last Updated: March 2017
Mandatory Revision Date: March 2018
Contact: Chief Information Officer (CIO)

Policy:
Carleton University provides secure remote access to many campus resources. This Policy establishes the baseline requirements necessary to provide a secure remote access service.

Purpose:
The purpose of this Policy is to define standards for connecting to any campus network or system from an off-campus location. These standards are intended to minimize the risk of damage to Carleton University. Damage may include unauthorized use, loss of data, disclosure of intellectual property; damage to public image, to internal systems, or any other undesired consequence.

Scope:
This Policy applies to all Carleton University students, faculty, staff, contractors, vendors, agents and other parties who access Carleton IT resources from off-campus locations using a Virtual Private Network (VPN).

This Policy applies to all Departments that provide remote access services.

All University Policies are to be adhered to, with the following providing specific direction:

- Acceptable Use Policy for Information Technology
- Information Security Policy
- Information Technology (IT) Security Policy

Procedures:
- ITS provides a centrally supported VPN service; when this central VPN cannot satisfy a departments specific needs then a departmental VPN service may be used
- Computers used for remote access must have an up-to-date anti-virus protection package installed and activated as well as firewall protection (hardware or software based)
- Remote Access solutions must use an industry standard IPSEC or SSL VPN solution, using strong encryption and centralized user authentication
- Unique credentials are required for each VPN user
• Processes and procedures must be in place to ensure user provisioning and de-provisioning exists and is aligned to HR termination procedures
• Remote access servers must offload logs to a central logging server and retain the logs for 90 days
• Remote access sessions must force a re-authentication of the user to the VPN service at least every 12 hours
• Remote access technologies used by vendors are activated only when needed, and are deactivated immediately after use
• Usernames and passwords for remote access must not be shared with anyone (including family members) for any purpose – University staff will NEVER ask you to disclose your username or password
• All University policies normally adhered to when on campus shall also be adhered to while off campus while using a VPN to the University
• Client VPNs must not store the password portion of VPN credentials, requiring the user to enter their password each time the VPN is established

Payment Card Industry Data Security Standards (PCI DSS) Requirements:
For IT infrastructure that is within the scope of PCI DSS compliance requirements, the following are also required:
• Sessions for remote access technologies must be automatically disconnected after 30 minutes of inactivity
• Remote access technologies used by third parties must only be activated when needed, and must be deactivated immediately after use
• Remote access must use ITS approved two-factor authentication
• It is strictly prohibited to copy, move or store cardholder data onto local hard drives and removable electronic media when accessing such data by remote access technologies

Roles and Responsibilities
Remote Users are responsible for:
• Conforming to Carleton University policies, procedures and standards when connecting to the University network
• Ensuring that their remote computer used to access University IT resources meets information security requirements
• Not saving or storing University confidential or sensitive data on non-University assets

ITS is responsible for:
• Implementing, maintaining and developing standards for remote access technologies
• Configuration and operation of VPN services in compliance with University Policy

Department Chairs, Directors and Management in all Departments are responsible for:
• Ensuring that VPN services configured within their Departments are done so in compliance with University Policy
• Ensuring that each VPN user is uniquely identifiable
• Ensuring that VPN logs are stored as per policy
• Ensuring that access granted through VPN services are terminated for departing individuals
• Ensuring firewall requests are submitted for any new systems as well as de-commissioned systems
• Participating in any internal or external audits that touch on remote access technologies
Department of Human Resources is responsible for:
  • Reporting employee departures to ITS to ensure that their remote access is disabled

**Compliance:**
Non-compliance to this Policy may result in disciplinary action.

**Contacts:**
Chief Information Officer, ITS

**Links to related Policies:** [http://carleton.ca/secretariat/policies/](http://carleton.ca/secretariat/policies/)
  • Acceptable Use Policy for Information Technology (IT)
  • Information Technology (IT) Security
  • Password Policy for Information Systems