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:	**September 2021**
Mandatory Revision Date:	**September 2022**
Contact:	**AVP (ITS) & Chief Information Officer**

Policy:
Carleton University requires that remote access to non-public and/or administrative data of the on-campus network use necessary safeguards to protect the confidentiality, integrity and availability of the data.

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 faculty, staff, students, contractors, vendors, agents and other parties who access non-public and/or administrative 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
- Data and Information Classification and Protection Policy
- Information Technology (IT) Security Policy
- CUNET Domain Membership and Access Policy

Procedures:
A Virtual Private Network (VPN) provides secure access to a remote network. Accessing the Carleton network via a VPN connection places your computer or device on the network as if it was directly connected while on-campus. As such, this can introduce various risks to the confidentiality, integrity and availability of the information and services that Carleton provides. The requirements to offer and use VPN services at Carleton include:

- 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 endpoint security solution installed and activated as well as firewall protection (hardware or software based). Remote Access solutions must use an industry standard IPSEC or SSL/TLS 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 Human Resources termination procedures.
- Authentication systems must offload logs to a central logging server and retain the logs for at least 180 days.
- 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 requires the use of two-factor authentication and 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.
- Client VPNs must not store the password portion of VPN credentials, requiring the user to enter their password each time the VPN is established.
- Remote access to sensitive areas of the Carleton network may require the use of two-factor authentication when authenticating to a VPN.

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.
- Using two-factor authentication, where possible, when using University IT resources.

ITS is responsible for:

- Implementing, maintaining and developing standards for all remote access technologies.

- Configuration and operation of VPN services in compliance with University Policy.
- Evaluating whether two-factor authentication is required on accounts used for remote access or VPN.
- Ensuring that University department's received a "go" security assessment prior to any new VPN or remote access service being brought online.

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 and received a "go" security assessment prior to their implementation.
- Ensuring that each VPN user is uniquely identifiable.
- Ensuring that VPN and authentication system logs are stored as per policy.
- Ensuring that access granted through VPN services are terminated for departing staff, faculty, student affiliates, and 3rd parties when no longer required.
- Ensuring firewall requests are submitted for any new systems as well as de-commissioned systems.
- Ensuring that two-factor authentication is integrated into systems in accordance with university policy.
- Participating in any internal or external audits that involve 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:
Assistant Vice-President (ITS) & Chief Information Officer

Links to related Policies: http://carleton.ca/secretariat/policies/

- Acceptable Use Policy for Information Technology (IT)
- Information Technology (IT) Security
- Password Policy for Information Systems
- CUNET Domain Membership and Access Policy
- Information Security Incident Response