



Canada's Capital University

<b>Policy Name:</b>	Internet Bandwidth Management
<b>Originating/Responsible Department:</b>	Information Technology Services (ITS)
<b>Approval Authority:</b>	Chief Information Officer (CIO)
<b>Date of Original Policy:</b>	August 2012
<b>Last Updated:</b>	August 2012
<b>Mandatory Revision Date:</b>	August 2017
<b>Contact:</b>	Director, Operations and Infrastructure, ITS

**Policy:**

This Policy outlines the Internet Bandwidth Management being used in the University.

**Purpose:**

The purpose of this Policy is to ensure the delivery of reliable internet service with sufficient capacity to support the academic, administrative and research functions of the University. Without internet bandwidth management, uncontrolled recreational activities would rapidly consume available internet bandwidth, and will put mission critical applications at risk to the point of not being usable.

**Scope:**

This Policy applies to any user communicating to and/or from the internet via the Carleton University campus, regardless of their affiliation with the University.

**Procedures:**

**Internet Connection and Capacity**

ITS manages multiple internet connections supplied by diverse Internet Service Providers (ISP). These multiple internet connections provide resiliency and capacity to meet the continuously growing internet bandwidth requirement of the University.

**Traffic Control Strategies**

The University has deployed traffic management technologies to allow the allocation of bandwidth based on policy rules. These technologies allow the allocation of bandwidth to specific types of internet traffic by assigning priority rules, rate limits, or both, to each type of internet traffic. The bandwidth allocation for campus relies on the priority allocation of bandwidth. An extensive list of commonly used network applications has been developed based on observed usage patterns and/or requests made by members of the user community via the ITS Service Desk.

Most commonly used applications such as HTTP, HTTPS, TELNET, SSH, and many others are provided priority.

If the traffic shaping devices encounter a type of network traffic that does not have a defined rule and policy for bandwidth allocation, this type of traffic is still allocated bandwidth, but it will receive a non-priority allocation of whatever capacity is available after the prioritized applications have been serviced.

ITS fully acknowledges that there will be occasions where no rule may exist in the traffic management devices to meet a specific business requirement, and that the performance delivered to the application may suffer as a result. Users encountering this behaviour should open a service request through the ITS Service Desk to ensure that appropriate measures are taken to improve performance.

#### **Compromised Systems or Abusive Behaviour**

To ensure that internet traffic to and from the university community will not be affected by compromised systems, ITS may take steps to isolate these systems from the campus network. More information related to this can be found in the standard operating procedure - [Responding to a Network Abuse Related Incident Causing Network Service Degradation](#).

#### **Bandwidth Allocation Requests and Special Circumstances**

Departments that will require bandwidth allocation and prioritization based on special circumstances or for special events should submit request through the ITS Service Desk.

#### **Changes in the Internet Bandwidth Management**

ITS reserves the right to make changes in the Internet Bandwidth Management as the needs arise. These changes may include internet traffic prioritization, bandwidth tiers and capacity, technology platform and others. Any significant change will be added to this Policy.

#### **Compliance:**

Non-compliance with this Policy may result in disciplinary action.

#### **Contacts:**

Director, Operations and Infrastructure, ITS

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

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