Ver 1 2017Mar03

DRAFT IT REMOTE ACCESS POLICY

PURPOSE

The purpose of this Policy is to define requirements for remote connectivity to Brock University's systems, services and data that are not explicitly publically accessible using any device, regardless whether the device is University- or personally-owned. This is to minimize the potential exposure to Brock University of damages which may result from unauthorized use of Brock resources.

SCOPE

This Policy applies to all employees (i.e., faculty, staff), students, consultants, vendors or any third party affiliate connecting remotely to Brock University's network via the University's provided remote access service. It does not apply to University applications explicitly made available through the internet (e.g., email, my.brocku.ca).

The scope of this Policy includes all users of remote access systems.

In the event that any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail.

POLICY STATEMENT

- All remote access not explicitly made public must be established by a secured and centrally managed service (e.g., Virtual Private Network (VPN), Remote Desktop Service, Remote Application Publishing) that complies with the Standards for Remote Access
- Users are not permitted to be connected to multiple networks while using remote access services (i.e., no split tunneling when using a VPN)
- Server logs of all remote access services must be retained for a minimum period of 90 days for review / audit.

- Multi-factor authentication is required for users and/or destinations, as determined by ITS risk assessment.

DEFINITIONS

Remote Access: Access to Brock University systems from an untrusted network zone (e.g., Internet, DMZ, ResNet).

Remote Access System: A service (e.g., VPN) which provides remote access to non-public Brock University systems and services.

Virtual Private Network (VPN): A secured private network connection built on top of a public network. VPN provides a secure tunnel over the internet between a computer and a private network.

COMPLIANCE AND REPORTING

Information Technology Services ("ITS") enforces this Policy and the related Standards at all times. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy must promptly report it to the ITS Help Desk. Policy violations that come to the attention of the ITS Help Desk will be escalated to the Director, Infrastructure.

Policy violations will be assessed and action taken to remediate the violation, subject to collective agreements and / or other contractual conditions.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the Associate Vice-President, ITS for further action. Periodically, the AVP, ITS will provide to SAC a summary of all policy violations.

Policy owner:	Associate Vice-President, Information Technology Services
Authorized by:	Board of Trustees, Capital Infrastructure Committee
Accepted by:	SAC
Effective date:	March 2017
Next review:	March 2018
Revision history:	2016

Related documents:	• Standards for Remote Access • Logical Access • Acceptable Use