Ver 1 2017Mar03

IT REMOTE ACCESS STANDARDS

PURPOSE

This document outlines requirements that must be adhered to when using, deploying and administering remote access services to connect to Brock University's systems and data from an untrusted zone (e.g., Internet). This document contains requirements that are specific to usage, administration, setup, maintenance and configuration.

Virtual Private Network (VPN) and Remote Access Services (RAS)

Virtual Private Networking ("VPN") and Remote Access Services ("RAS") open a door to Brock's network and extend the University's network to the remote computer. It is imperative, therefore, that these services be centrally reviewed, monitored and approved.

Only remote access services that comply with the requirements in this document will be permitted to connect to Brock's network. Non-compliant remote access services will be reported to Director, IT Infrastructure. The administrator will be required to implement appropriate controls or the solution will be shut down. Any investigation of reported violations will be carried out in accordance with collective agreements and / or contractual conditions.

All systems and services not purposely made public available through the internet by ITS must be accessed through a remote access service.

Published Services

Requests to make new services publicly accessible must be submitted via an ITS Help Desk support request for review, risk assessment and change control scheduling.

These changes must be made in compliance with the IT Firewall Policy and related Standards.

Identity Authentication

The identity of a user connecting via a remote access service must be authenticated upon initiation of each session. Automated logins are not permitted.

All remote access services must authenticate users against the Campus Active Directory.

Multi-factor authentication is mandatory for some service endpoints, based on ITS risk assessment and/or relevant requirements. (e.g., PCI compliance requires MFA for administrative access).

Remote Access Sessions

Termination of remote access sessions must occur after an inactivity period of 60 minutes in order to reduce the possibility of unauthorized users accessing unattended devices.

Split tunneling must be disabled so that devices connected to Brock's network cannot be connected to other networks at the same time.

Remote Computing Devices and Software

Remote devices must be operated in accordance with, and maintain a level of security commensurate with, that enforced on devices connected to the local area network.

To achieve this principle, all users connected via remote access services must (if technically supported):

- Have vendor supported operating system and software that is up to date;
- Be protected with a personal or desktop firewall;
- Be protected with antivirus/anti malware software with signatures that are automatically updated.

Users requiring assistance / clarification are strongly encouraged to contact / visit the ITS Help Desk.

Remote Access Services for Brock Users

Active staff, faculty and students are eligible for remote access.

Staff and faculty user accounts are automatically granted remote access rights to core services on Brock's public network.

Access to resources on the private network must be requested using the Security Access Request Form.

Course instructors must request remote access on behalf of their students for the duration of the course if they need to access networked resources not available through normal means. This is done via a Security Access Request Form.

Monitoring

A central remote access log must be maintained by ITS and retained for a minimum period of 90 days.

Remote Access Usage

The log must contain successful and failed login attempts.

Remote Access Implementation

Equipment used to provide and support remote access gateways must:

- Terminate in a DMZ;
- Be hardened with updated patches and antivirus.

Administrative access to remote access services must be limited to authorized and trained technical staff whose identity is authenticated using Campus Active Directory. (i.e., no local user accounts).

Remote access services which are not managed by ITS will be reviewed and monitored for compliance with this Policy and related Standards.

Requesting a new remote access service

New remote access services can be requested by creating a Schedule 8 project request.

Remote Access Security Assessments

Remote access infrastructure is a boundary level control for the entire Brock network and therefore must be reviewed for security posture and assessed regularly, particularly when there is significant change to the technology, physical design or other elements that may introduce new threats or vulnerabilities. This assessment will be conducted by the ITS infrastructure team as part of the change management process.

RESPONSIBILITIES

Remote Access Users

All Remote Access users are responsible for:

- Adhering to the Remote Access Policy and related Standards and the University's IT Acceptable Use Policy;
- Ensuring that security safeguards installed to protect their remote device are not deliberately disabled;
- Exercising good judgment and having awareness of key cyber security issues;
- Avoiding use of public terminals;
- Protecting Brock University systems and data from unauthorized individuals;
- Reporting any suspected security breaches to the ITS Help Desk; and

- Contacting the ITS Help Desk for assistance as required.

Remote Access Administrators

Remote access administrators are responsible for:

- Ensuring that a request for termination of remote access privileges is promptly acted upon
- Monitoring the administration, operations and security of the remote access infrastructure for adherence to these requirements
- Ensuring that security testing and evaluation of the remote access gateway is completed whenever there is a change that could introduce new threats or vulnerabilities.

Definitions

Demilitarized Zone (DMZ): A DMZ is a computer host inserted as a neutral zone between an organization's private network and the outside public network. It prevents outside users from getting direct access to organizational data.

Remote Access: Access to a Brock University system from an untrusted zone (e.g., Internet).

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

Remote Desktop: A program or operating system feature that allows the user to connect to a computer in another location.

Secure Shell (SSH): A secure shell user for remote command line login, remote command execution and other secure network services between networked computers.

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.