IT SYSTEM SECURITY POLICY

PURPOSE

The purpose of this Policy is to outline the requirements for installation, maintenance and operation of information technology ("IT") systems in a secure fashion in order to prevent unauthorized system use and to ensure data and system security.

SCOPE

This Policy applies to all Brock IT servers, software and network infrastructure (systems) regardless of location.

If any provision of this Policy is found to be inconsistent with the provisions of a collective agreement, the collective agreement will prevail, unless the Policy provision is required by law, in which case the Policy provision will prevail.

POLICY STATEMENT

All Brock systems and services must adhere to the technical standards set out in the "Standards for System Security" document, as outlined below:

- Unnecessary software services must be deactivated or de-installed;
- All default user passwords and, if possible, account names must be changed;
- All default SNMP community strings must be changed upon installation;
- Upon deployment and at least annually thereafter, all systems must be reviewed for known vulnerabilities and remediated. If the vulnerability is critical and cannot be remediated it must be reported to the Director, Infrastructure;
- Systems must remain on a supported and patched version;
- All systems must be protected by anti-virus, and anti-virus must be kept up to date;

- All systems must reside in a data center or in a physically secure managed location;
- Physical access to servers and systems must be limited by job function;
- Vulnerability scans must be performed on systems upon initial implementation and thereafter on a regular basis;
- Security logs for critical systems must be managed via a centralized logging solution and retained and reviewed on a regular basis;
- Systems that are not in compliance with this Policy and related Standards for System Security may be terminated at the discretion of the Associate Vice-President ("AVP"), Information Technology Services ("ITS").

Exceptions to this Policy must be documented and presented to the AVP, ITS for final approval.

DEFINITIONS

Application: a computer program designed for a specific task or use

Server: a computing device capable of accepting requests from a client and giving responses accordingly

Simple Network Management Protocol (SNMP): A protocol for network management used for collecting information from and writing to network devices

Systems: Servers, services and/or applications**,** or network devices

COMPLIANCE AND REPORTING

ITS enforces this Policy and related Standards at all times. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to 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 agreement and / or other contractual conditions.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the AVP, 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:	Current version: Executive Team Prior versions: Board of Trustees, Capital Infrastructure Committee
Approved by:	SAC
Effective date:	December 2021
Next review:	December 2022
Revision history:	2020 2017 2016
Related documents:	• IT System Security Standards (ITS only) • IT Acceptable Use Policy