IT ACCEPTABLE USE STANDARDS

PURPOSE

A standard includes specific low level mandatory controls that help enforce and support a policy.

The purpose of this document is to support and outline in detail the requirements of the IT Acceptable Use Policy. These requirements are mandatory and must be adhered to by all users of Brock University's information technology resources, including employees (i.e., faculty, staff), students, visitors (e.g., visiting scholars, guests, other 3rd parties), contractors, consultants, etc.

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

STANDARDS

Brock University IT resources are provided for University-related purposes, including support for the University's mission of teaching, research and its administrative functions.

Technology resources are also provided to enhance student and campus life activities in student residences, general access computer labs, teaching labs and to on-campus vendors and visitors.

All users of Brock University information technology resources are required to comply with the following:

Security

Users must register their systems with the ITS Help Desk for LAN/ cable internet.

Users are responsible for all activities on machines that are registered to them and are accountable for all use.

Users must not circumvent security or exploit security vulnerabilities at Brock University.

Sniffing or other forms of network wiretapping is prohibited.

Passwords

Users must keep their passwords confidential and secure. Users must not allow others to access their accounts.

Users must ensure that all passwords comply with Brock University's password parameters as outlined in the End User Logical Access Standards.

Malware

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors, etc.) being imported into Brock University's network and systems.

All Brock University-owned devices must have licensed virus and malware protection software installed with all current updates applied, and must not be deactivated by the user.

As outlined in the Safe Disclosure Policy, users are encouraged to report any actual or suspected malware infection immediately by calling or visiting the ITS Help Desk (x4357).

Software

The University respects intellectual property and does not tolerate the unauthorized copying of software, including programs, applications, databases and code. Copying of any University-owned computer software is prohibited.

Email

Use of email by Brock University employees and students is permitted and encouraged where such use is suitable for University purposes and supports the goals and objectives of the University.

Use of email for the following types of activities is prohibited:

- Unauthorized upload, download or transmittal of commercial software or any copyrighted materials;
- Harvesting or generating spam (i.e., unsolicited commercial electronic messages as defined by the Canadian Anti-Spam Legislation) to any email recipients;

- Sending any material that is obscene, unless it is done for the sole purpose of teaching, research, or service, as protected under relevant collective agreements, or defamatory or which is intended to annoy, harass or intimidate another person;
- Distributing, disseminating or storing images, text or materials that may be considered indecent, pornographic, obscene or illegal unless it is done for the sole purpose of teaching, research, or service, as protected under relevant collective agreements;
- Forging, misrepresenting, obscuring, suppressing or replacing a user identity on any electronic communication to mislead the recipient about the sender;
- Sending "mass email" type messages to the University community without approval. Prior approval is required from Marketing and Communications.

Brock-owned equipment

Users supplied with computer equipment by Brock University are responsible for the safety and care of this equipment as well as the security of software and data stored on the equipment.

Users must not install unlicensed or unauthorized copies of computer software on University-owned computer equipment.

Portable devices

Institutional data on portable devices, such as laptops, tablets, smartphones and electronic storage devices, is especially vulnerable. Accordingly, particular care must be exercised with these devices. This includes:

- Locking the device with a complex password;
- Locking an idle device with a password (time-out configuration);
- Physically securing the device when not in use;
- Ensuring laptops and tablets are protected with anti-virus software at all times;
- Ensuring data on electronic storage devices is encrypted;
- Remote erasure of a device if lost/ stolen/ misplaced as outlined in the Remote Erasure Procedures.

Users are responsible for the consequences of theft or disclosure of information on portable devices if they have not taken reasonable precautions to secure the device. Policy violations will be assessed and action taken to remediate the violation, including consequences where appropriate, subject to collective agreements and / or other contractual conditions.

The loss or theft of a portable computing device or portable electronic storage media within the scope of this Standard must be reported to the employee's administrator/ manager/ supervisor.

The administrator/ manager/ supervisor must inform Campus Security and the ITS Help Desk immediately upon such notification.

Workstations

All workstations (including desktops / laptops) must be secured with a lock-on-idle policy after 20 minutes of inactivity.

In addition, the screen and keyboard should be manually locked by the user when leaving the machine unattended (Ctrl + Alt + Delete → Lock this computer).

Wireless

Wireless users must adhere to the following:

- The privacy of other wireless users is paramount; wireless sniffers are prohibited;
- Interference with functionality or activities that deny wireless use are prohibited.

Personal wireless hubs are prohibited as they may allow unauthorized individuals to access the Brock network and/ or degrade overall network performance.

A user registering a personal wireless router in a student residence without University-provided wireless access is responsible for violation of copyright infringement originating from devices connecting to the wireless router.

Exceptions to the requirements outlined above must be discussed beforehand with the Director, Client Services, Information Technology Services.