END USER LOGICAL ACCESS POLICY

PURPOSE

The purpose of the End User Logical Access Policy is to safeguard Brock University's systems and maintain ongoing data integrity by allowing access to Brock's systems and data only to authorized users.

While physical access controls provide protection through physical means (e.g., walls, locks, cameras, etc.), computer-based access controls (i.e., logical access controls) protect IT systems and electronic data by verifying and validating authorized users, authorizing user access to IT systems and data and restricting transactions (read / write / execute / delete) according to the user's authorization level.

SCOPE

This Policy applies to all authorized users including Brock employees (i.e., faculty, staff), students, contractors and visitors who may have access to Brock IT infrastructure or services.

In terms of technology, this Policy applies to the Brock communications, network and document management infrastructure and related applications, including all systems, services and supporting infrastructure at all sites where Brock University's electronic information is collected, processed, transmitted, stored and / or deleted.

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

The integrity of Brock University's technology and data must be maintained by protecting access to IT systems and applications and preventing unauthorized access to these resources.

Access to Brock University systems is restricted to only authorized users or processes, based on the principle of least privilege.

Logical access controls are categorized in the following manner and are detailed in the End User Logical Access Standards:

- Account management;
- Password management;
- Monitoring and oversight.

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 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 referred to the Director, Client Services.

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.

Where Policy violations are considered severe and / or cannot be easily remediated, the incident will be escalated to the Associate Vice-President (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:	Board of Trustees, Capital Infrastructure Committee
Accepted by:	Senior Administrative Council
Effective date:	June 2020
Next review:	June 2022
Revision history:	2019 2017 2016
Related documents:	End User Logical Access Standards Privileged Users Logical Access Policy IT Acceptable Use Policy and related Standards