DATABASE ACCESS POLICY

PURPOSE

The purpose of this Policy is to preserve the confidentiality, integrity and availability of the University's information assets by restricting access to enterprise application databases that store Brock's data.

SCOPE

This Policy applies to all employees and all enterprise applications, as identified by the Information Technology ("IT") Service Catalogue, which supports Brock University.

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

Direct access to enterprise application databases ("Databases") will be limited to Information Technology Services ("ITS") staff and enterprise applications in the following way:

- Direct access to Databases by ITS staff is restricted to the lowest level of user rights possible while still maintaining the employee's ability to perform their job duties.
- Direct access to Databases by enterprise-level mission critical applications will be restricted to the minimal level that allows normal functioning.

Responsibility

This Policy is under the jurisdiction of ITS Enterprise Solutions.. Final decisions related to this Policy will be made by Director, Enterprise Solutions, where required.

DEFINITIONS

Application. The use of information resources (information and information technology) to satisfy a specific set of user requirements. An application can refer to a functional category such as admissions, payroll or registrations.

Database. A set of related files that is created and managed by a database management system (DBMS).

COMPLIANCE AND REPORTING

Database access is reviewed on an ongoing basis by the information security team. Every effort will be made to correct identified access-related events in conflict with this Policy without interrupting normal University operations.

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 report it promptly to the IT Security Specialist. Policy violations that come to the attention of the IT Security Specialist will be escalated to the Director, Enterprise Solutions.

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 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
Accepted by:	Senior Administrative Council
Effective date:	May 2022
Next review:	June 2025
Revision history:	2022 2019 2017 2016
Related documents:	Database Access Standard Logical Access Policy and related Standards IT Service Catalogue