DATABASE ACCESS STANDARDS

PURPOSE

The purpose of this document is to support and outline in detail the requirements of the Database Access Policy. These requirements are mandatory and must be adhered to by all employees and all enterprise applications that support Brock University.

Access: ITS Staff

Database access by Information Technology Services ("ITS") staff must adhere to the following requirements:

- Use an elevated privileges *CAMPUS* domain account
- Use an authenticated *CAMPUS* client computer
- Client computer must use the following (see Logical Access Policy and related Standards):
  - Authorized network connection
  - IP address in the designated *ITS* private address range
  - Authorized access through the network firewall and application firewall
- Use authorized and managed client applications.

Database access by ITS staff is broken down into the following functional groups:

- Application Developers ("AD")
- Business Systems Analysts ("BSA")
- Database Administrators ("DBA")
- System Administrators ("SA").

Database access is broken down into the following functional server environments:

- Production ("PROD")
- Quality Assurance ("QA")
- Test and Development ("DEV").

ITS staff functional group database access must have the following environment permissions in place:

Environment:	PROD	QA	DEV
AD	None	None	Full control *
BSA	Read only *	Read & write *	Full control *
DBA	Full control	Full control	Full control
SA	Full control	Full control	Full control

* Access limited weekdays from 7:00 a.m. to 7:00 p.m.

In situations where ITS staff functional groups do not exist, the rule of least privilege in order to perform job functions must be observed.

Access: Applications

Database access by applications must adhere to the following requirements:

- Must use an authorized *CAMPUS* domain account or authorized database account (i.e., batch and service accounts)
- Authorized accounts must be requested and approved through the Security Access Request Form
- The IT application account must meet the following requirements:
  - Must not be shared between IT applications
  - Must be created using the least set of privileges.

Access – Database objects

Access to database objects (stored procedures, functions, schemas, etc.) must be limited to ITS staff.

Exceptions to these Standards must be documented and approved by the Director, Enterprise Solutions.