SOFTWARE DEVELOPMENT POLICY

PURPOSE

The purpose of this Policy is to standardize software development for all enterprise-level centrally-managed mission critical web applications and web services through the use of industry leading practices. These applications and services typically deal with sensitive data and / or HR-, finance-, donor-, student admission-, student record- or course related data, and due diligence in protecting this data is required. Standardizing the development approach and coding techniques for critical systems will ensure their maintainability, security, protection against cyber-attacks and accessibility.

SCOPE

This Policy applies to all employees (i.e., faculty, staff), consultants and / or contractors involved in the development or modification of enterprise-level centrally-managed mission critical applications that support 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

Information Technology Services ("ITS") is responsible for developing, maintaining, and participating in a System Development Life Cycle ("SDLC") for Brock web projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this Policy addresses the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; design specification; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for sensitive Brock information.

All enterprise-level centrally-managed mission critical applications developed at or for Brock University must adhere to development standards and procedures documented in the

ITS Application Development Standards guide. These standards include: coding techniques, testing strategies, documentation requirements and software release processes that align with industry standards and regulatory requirements.

There must be a separation between the production, development and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems.

Responsibility

This Policy is under the jurisdiction of ITS Application Development. The interpretation and application of this Policy is the responsibility of the Application Architect. Final decisions related to this Policy will be made by Director of Application Development, where required.

DEFINITIONS

Application. Computer programs, procedures, rules and associated documentation and data pertaining to the operation of a computer system.

Mission Critical. A system or application whose failure will result in the failure of University operations.

System Development Life Cycle (SDLC). A standardized process for planning, creating, testing, and deploying an application.

COMPLIANCE AND REPORTING

All applications are reviewed at predetermined checkpoints of the SDLC by the Application Architect or their designate. Any deviations are identified and corrective action is determined prior to the application being released to production.

Electronic authorization indicating standards have been met is required before a new or modified application can be released to production.

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 escalated to the Director, Application Development.

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 Associate Vice-President, 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:	Senior Administrative Council
Effective date:	May 2022
Next review:	June 2025
Revision history:	2015 2016 2017 2019 2020
Related documents:	Software Development Standards System Integration Standards Payment Card Industry Data Security Standard (PCI DSS): https://www.pcisecuritystandards.org/security_standards/documents.php