PRIVILEGED USERS LOGICAL ACCESS POLICY

PURPOSE

This Policy informs system and application administrators at all levels of the inherent obligations and responsibilities that accompany privileged access as well as the approvals required for granting, reviewing and revoking privileged access.

SCOPE

This Policy applies to all Brock University employees with privileged / elevated access to Brock University servers or services.

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

All requests for changes / deletions / additions to a user's privileged access must be completed using the Security Access Request Form ("SARF"). Level 1 ("L1") and Level 2 ("L2") approval is required for all such requests, including the approval of the data owner.

All requests for vendor / contractor privileged access must be completed using the SARF, and this access must have an expiry date (i.e., temporary account). L1 and L2 approval is required for all such requests, including the approval of the data owner. The vendor must also complete the Brock University Confidentiality form.

Privileged access will be granted on the basis of least privilege.

Privileged access will be granted based on job description and will be restricted to users who need the elevated permissions to maintain a system or service.

Linux users with privileged access to enterprise level servers must login to a particular computer system using their own login

credentials and gain privilege through use of the "su" or "sudo" commands.

Users with privileged access must have two accounts: one for normal day-to-day operations and the other for administrator duties.

All privileged access to administrative systems must be done via multi-factor authentication (MFA).

Privileged users must not use their access for unauthorized viewing, modification, copying or destruction of system or user data.

Semi-annual reviews of privileged access must be conducted by the department responsible for the system / service. Privileged access no longer required must be immediately removed.

All privileged access account passwords must be immediately changed in the event of an employee termination or change of duties no longer requiring privileged access. This includes service accounts.

DEFINITIONS

Data owner. The person who can authorize or deny access to certain data, and is responsible for its integrity. A list of data owners is available on "one.brocku.ca" under the Information Technology Services ("ITS") site.

Least privilege. The minimum level of permissions necessary to perform a user's duties.

Privileged access. Access that allows the user non-standard or elevated privileges allowing access to administrate systems or data. This includes the ability to alter system configurations, manage software systems, grant access, etc. It also includes elevated access to University data enabling direct SQL querying, data management, data maintenance or reporting.

Server. A server is a software program, or the computer on which that program runs, that provides a specific kind of service to client software running on the same computer or other computers on a network.

Service. A means of delivering value to "customers" by facilitating outcomes customers want to achieve without the

ownership of specific costs and risks. Examples of services are email, networking and web hosting.

Service account. An account used to run an application software service or process or an account used to provide access between application software and data.

COMPLIANCE AND REPORTING

Compliance: This Policy is under the jurisdiction of the AVP, ITS. Each authorized user of the University's IT systems is required to comply with this Policy and related documents.

Exceptions to this Policy must be documented and authorized by the VP Administration and presented to ITS.

Incidents determined to be in non-compliance with this Policy will be assessed for severity and will carry a possible range of sanctions.

Reporting: The AVP ITS will provide to SAC a summary of policy violations as required.

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:	December 2021
Next review:	December 2022
Revision history:	2020 2019 2017 2016
Related documents:	IT Acceptable Use Policy Brock University Code of Conduct