IT SENSITIVE AREA PHYSICAL ACCESS POLICY

PURPOSE

The purpose of the IT Sensitive Area Physical Access Policy is to limit and control physical access to areas in the University where sensitive data is stored or areas which contain critical IT infrastructure assets. This Policy and the related Standards outline the responsibilities and practices to be carried out in order to protect Brock's critical assets and sensitive data from unauthorized access.

SCOPE

This Policy applies to all personnel who may require access to areas in the University where IT sensitive data is stored or areas which contain critical IT assets as outlined in the IT Sensitive Area Physical Access Standards.

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

Entry to all University space listed in the IT Sensitive Area Physical Access Standards must be controlled (monitored) through physical security systems such as video cameras, card (swipe or proximity) and/or keyed entry.

Access to critical IT Infrastructure assets is granted only to specific Brock University employees upon approval and to authorized contractors under the responsibility of Facilities Management:

- Access is granted to named individuals only and is based on job function. Group access is not permitted.
- Contractors must be admitted to IT sensitive areas by employees from Information Technology Services ("ITS"), Facilities Management or Campus Security.

- Authorized personnel must present identifying badges upon request when in an IT sensitive area. Badges must contain the individual's name, picture and company.

Visitors, including vendors / service providers that require temporary access to an IT sensitive area, may be permitted within an IT sensitive area only when escorted at all times by an employee from ITS, Facilities Management or Campus Security.

Access must be removed / revoked in a timely manner when no longer required.

Upon termination or changes in responsibility, all physical access mechanisms such as card access and keys must be disabled and returned.

Periodic reviews of the log activity and permission lists must be conducted by the Director, Infrastructure.

Lost or stolen access cards or keys must be reported immediately to the Director, Infrastructure.

COMPLIANCE AND REPORTING

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 ITS Help Desk. Policy violations that come to the attention of the ITS Help Desk will be referred immediately to the Director, Infrastructure or designate.

Policy violations will be assessed, and action taken to remediate the violation. These actions shall include appropriate consequences, subject to relevant collective agreements and / or other contractual conditions.

Where Policy violations are considered severe, or cannot be easily remediated, the incident will be referred to the AVP, ITS for further action. Periodically, the AVP, ITS will provide to SAC a summary of all known 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:	December 2021
Next review:	December 2022
Revision history:	2020 2019 2017 2016
Related documents:	IT Sensitive Area Physical Access Standards