Brock University

IT SENSITIVE AREA PHYSICAL ACCESS STANDARDS

PURPOSE

The purpose of this document is to support and outline in detail the requirements of the IT Sensitive Area Physical Access Policy. This Standard applies to all personnel who require access to areas in the University where IT sensitive data is stored or areas which contain critical IT assets.

SCOPE

The IT Sensitive Area Physical Access Policy applies to locations on campus which contain critical IT assets such as servers, network and telecommunications equipment.

Securing the area

All facilities with critical IT assets must be kept secured at all times. Appropriate facility entry controls include one or more of the following:

- Access control management system to validate and electronically log
- Key entry (with manual log and video camera)
- Keypad entry.

All personnel with authorized access must have their own individual alarm code. No shared credentials are permitted.

“Tailgating” or “piggybacking” (entry of 2 or more people under one access method) is prohibited.

IT sensitive area identification

All IT sensitive areas must be externally identifiable with signage displaying minimal information, e.g., “*Authorized Employees Only*”.

Access requests/ approval

All requests for authorized access to IT sensitive areas must be made through the Security Access Request Form.

Brock employee access

Brock University employees from various departments may be granted access to IT sensitive areas. This is at the discretion of the AVP, Information Technology Services and is based on the requestor’s job responsibilities.

Brock University employees do not require an escort. Employees must have valid Brock photo identification at all times when working within these facilities.

Non-Brock employee access

Visitors to IT sensitive areas who are not Brock employees must be escorted by a Brock employee at all times.

Facilities Management contractors requiring unescorted access to IT sensitive areas are restricted to pre-qualified vendors only with contractual agreements to deliver services that require such access.

First responders including police, fire or medical staff will be granted access in an emergency by Campus Security.

Generic / shared access

Generic or shared access codes and proximity cards must not be used. Sharing of keys or proximity cards is not permitted.

Training requirements

Certain IT sensitive areas contain fire suppression systems. No access to these IT sensitive areas will be approved until the individual(s) has undergone a training session on the fire suppression system.

Revoking access

The Director, Infrastructure or designate must ensure the timely revocation of access to IT sensitive areas when the access is deemed to be no longer required.

Access review

Semi-annually, access permissions to the IT sensitive areas as well as the entry logs (electronic and visitor access logs) must be reviewed. The reviews will be retained for one year.

Deficiencies must be reported to the AVP, ITS, and remedial action taken, including, but not limited to the removal of access.

Lost / stolen card or keys

Lost or stolen card or keys must be reported to the Director, Infrastructure or designate and access removed.