Carleton University

Canada's Capital University

Policy Name:	Data Centre Access
Originating/Responsible Department:	Information Technology Services(ITS)
Approval Authority:	Chief Information Officer (CIO)
Date of Original Policy:	October, 2008
Last Updated:	October, 2013
Mandatory Revision Date:	October, 2018
Contact:	Director, Operations and Infrastructure, ITS

Policy:

Carleton's Data Centres house the University's infrastructure that includes but is not limited to the campus network, information security, the enterprise administrative systems, and Library systems. These centres are located in Robertson Hall and the MacOdrum Library; and are managed by the Department of Information Technology Services(ITS) and the University Library.

This Policy addresses Information Technology (IT) security issues with regards to staff and other personnel's physical access to the Data Centres.

Purpose:

The purpose of this Policy is to define the standards for the granting, controlling, monitoring, and removing of physical access to the Carleton University Data Centres. Effective implementation will minimize the risk associated with unauthorized access, and provide a method of auditing physical access.

Scope:

This Policy applies to:

- The primary Data Centre in Robertson Hall (RO) Room 406
- The Library Data Centre (LDC) in the MacOdrum Library (ML) Room 345
- Individuals who are granted physical access to the Robertson Hall Data Centre and the Library data centre whose names appear on the RO and/or the LDC "Access List"

Access related to logical systems (non-physical access) is not part of the scope of this Policy.

Procedures:

Data Centre – Robertson Hall (RODC)

Access to the RODC will be granted to employees whose daily work functions necessitate physical access to the facility. This includes: system administrators, security administrators and networking staff whose work responsibilities require that their work must be performed at the physical server location. Requests for access must be made to the ITS Security Administrator.

- Access to the RODC is granted via a Campus Card and a PIN
- PIN codes and Campus Cards must not be given out to any unauthorized persons and should be held in the strictest confidence
- Any person not on the access list needs to be escorted at all times by the responsible contact person(s)
- Contractors (other than those identified in the list) are to be escorted while in the RODC - anyone who grants access to Contractors or other visitors is responsible for their supervision – exceptions will be considered on a case by case basis
- Each individual that is granted access to the RODC will receive training on the use of the alarm system, as well as training on emergency procedures in case of activation of the Fire Suppression system
- No one is to attempt to keep the Data Centre doors open using chairs, books, or other objects
- The person(s) responsible for the RODC will review access rights on a term basis and remove access for individuals that no longer require access
- Absolutely no food or beverages are allowed in the RO Data Centre at any time

Library Data Centre (LDC) – MacOdrum Library (ML)

Access to the LDC will be granted to employees whose daily work functions necessitate physical access to the facility. This includes: system administrators, security administrators and networking staff whose work responsibilities require that their work must be performed at the physical server location.

A list of specified users that have access to the LDC will be maintained by the Security Administrator. An up-to-date copy of this “Access List” will be provided by email, each time a revision is made, to the following:

- Supervisor of Operations, ITS
- Information Systems Analyst/Network Administrator, Library
- Department of University Safety

Access to the LDC may be granted to others whose work function requires occasional access, such as vendor maintenance staff, Facilities Management and Planning maintenance staff, and other individuals known to those on the LDC “Access List”.

Granting, controlling, and monitoring of physical access to the LDC is subject to the following:

- Access to the LDC will be granted to ITS and Library staff members who are individually named in the “Access List”
- The LDC will be protected by multiple layers of physical security, including a monitored alarm system with motion detection
- Only those individuals named in the “Access List” will be provided a key to the LDC, and an alarm system code unique to them
- An LDC key can be borrowed from the Supervisor of Operations
- Alarm system codes and keys will not be shared or loaned to others
- Requests for additions to the “Access List” must be made by email to the person(s) responsible for the LDC: ITS Security Administrator and the Library Information Systems Analyst/Network Administrator
- Each individual that is granted access to the LDC will receive training on the use of the alarm system, as well as training on emergency procedures in case of activation of the fire suppression system

- The person(s) responsible for the LDC will review the access logs on a periodic basis and investigate any unusual access
- The person(s) responsible for the LDC will review alarm code and key access rights on a term basis and remove access for individuals that no longer require access
- Visitors to the LDC will be escorted at all times – those on the "Access List" are responsible for ensuring that persons they escort into the LDC follow appropriate procedures
- Exceptions for unescorted access may be made on a case-by-case basis when warranted, but only when authorized in advance by the person(s) responsible for the LDC
- The main point of entrance for authorized ITS staff will be the door adjacent to area ML301
- Both of the LDC doors must remain locked at all times
- Lost or stolen keys must be reported immediately to the person(s) responsible for the LDC
- Absolutely no food or beverages are allowed in the LDC at any time

Compliance

Non-compliance with this Policy may result in disciplinary action.

Contacts:

Director, Information Security, ITS
Director, Operations and Infrastructure, ITS
Head, Systems, University Library

Links to Related Policies:

N/A