1. Rationale

This policy is a recommendation for dealing with access to secured physical areas housing servers, storage devices, computers, network devices and other critical infrastructure computing components that support current services. Too often physical security is overlooked by operations staff as an afterthought; physical security and compliance with guidelines can be costly and yield low benefits to all but the site's operational staff. Procedures pertaining to security can be difficult to follow and maintain as new technologies are deployed at the site. The implementation of any policy or guideline requires a methodical set of procedures to be developed for assisting all those affected.

2. Access Authorization Requests

A central point of contact is assigned for each data center, network closet or operations facility. These contacts are delegated by the responsible director or manager claiming responsibility for the physical area, and maintenance thereof. A list of the current points of contact is available by calling ext. 7777 (TSC Helpdesk).

2.1 Requesting Access

An individual requiring physical access to a restricted area must obtain the necessary form for access to the physical location http://helpdesk.lakeheadu.ca/files/dataCentreAccess_form.pdf. A completed form must be sent to the appropriate contact(s) for the area prior to access being granted.

2.2 Reservation of Access Rights

Each Data Centre Access Request Form includes a disclaimer that access to secured area may be revoked temporarily or permanently for any reason, at any time.

Unescorted Access – you must have a approved, current Access Form approved and you must have been fully trained in the Data Centre's Fire Suppression System.

Escorted Access – Must be escorted by a TSC Staff member or an approved applicant that has been fully trained in the Data Centre's Fire Suppression System. Not adhering to this requirement may result in immediate removal of access to the TSC secure areas.

2.3 Emergency Access

Emergency access to a secured site will be an exception. Each applicant should have primary and secondary authorized personnel "on call" ready to respond to a situation at all times. Proper

cross-training and contact information should be developed to promote limiting of emergency access completely. *** TSC policy re call in

Glossary of Definitions

TSC	Technology Services Centre
Braun Data Centre	Refers to the Data Centre located in the Braun Building – BB1045
ATAC Data Centre	Refers to the Data Centre located in the ATAC Building – AT2007
Customer	Refers to an organization that has equipment connected in either of the TSC Datacenters
Sanctioned User	Individual representing a customer that has completed and been granted access to the Datacentre by TSC.
Vendor/ Sanctioned users	Refers to individuals that are not employed by the TSC or its customers, who are identified in writing by the customer on the TSC Data Centre Access Request Form, commonly referred to as third (3rd) party.
Licensed Area	Refers to that portion of the Data Centre made available by TSC to the Customer for the placement of Customer's equipment and use of the Data Centre Services

Site Access

1. Only those sanctioned users identified in writing by the customer on the TSC Access Request form may enter the DATA CENTRE.

2. For every DATA CENTRE visit, a maximum of 3 persons, of whom at least one must be a sanctioned user, may enter the DATA CENTRE at the same time. For security reasons, all visitors (sanctioned users and accompanying persons) will be required to show his/her STAFF ID for verification if requested. He/she will be refused to enter the DATA CENTRE if the required credentials cannot be shown.

3. TSC reserves the right not to allow entrance to the DATA CENTRE if the DATA CENTRE already has too many companies performing work.

4. Customer shall deliver prior written notice to TSC of any changes in the list of sanctioned users through the TSC Access Form.

5. Customer and its sanctioned users may only enter its licensed area, unless otherwise approved and accompanied by authorized TSC staff.

6. Customer has full responsibility and liability for all acts or omissions of sanctioned users and accompanying persons and such acts or omissions will be attributed to customer for all purposes, including for the purposes of determining whether customer has breached this policy.

7. Each customer must ensure that the sanctioned users and the accompanying person do not take any actions that customer is prohibited from taking under this policy.

8. Customer must provide TSC with at least (3) three working days prior notice any time it requires on site TSC technical support at the TSC DATA CENTRE or it intends to move-in or move-out any Customer equipment.

9. The sanctioned users and the accompanying persons must wear their staff ID cards and/or visitor cards within the TSC datacentres.

10. All visits by Customers and their sanctioned users and guests must register in the TSC Data Centre log book, including names and contact information.

Conduct at the DATA CENTRE

1. The Customer and sanctioned users installing or moving any of their equipment must review the plans with the designated TSC contact person to facilitate correct power and environmental requirements.
2. The sanctioned users and the accompanying persons must keep its licensed area as well as TSC DATA CENTRE clean and tidy at all times – they are responsible to leave the DATA CENTRE as they found it. The sanctioned users and the accompanying persons agree to adhere to and abide by security and safety measures established by TSC. The sanctioned users and the accompanying persons must refrain from doing the following:
3. Engage in any activity that is in violation of the laws or aids or assists any criminal activity while at TSC proper in connection with the DATA CENTRE services
4. Misuse or abuse of any TSC property or equipment or third party equipment;
5. Make any unauthorized use of or interfere with any property or equipment of any other customer
6. Harass any individual, including TSC personnel and sanctioned users of other customers
7. Use of any photographic, video, film or such other devices that produces, reproduces, retains or transmits images within the premises and the licensed space.
8. Customer must not except as otherwise agreed by TSC
9. Place any computer hardware or other equipment in the licensed area.
10. Store any paper or packaging products or other combustible materials of any kind in the licensed area and,
11. Bring any “prohibited materials” (as defined below) into the DATA CENTRE. Prohibited materials shall include but are not limited to the following and any similar items:
    a. food, drink, illegal drugs and other intoxicants
    b. tobacco products

c. explosives and weapons

d. hazardous materials

e. electro-magnetic devices, which could unreasonably interfere with computer and telecommunications equipment

f. radioactive materials

g. photographic or recording equipment of any kind

h. any other items deemed inappropriate at TSC sole discretion

12. All of Customer's equipment must be installed, operated, configured and run at all times in compliance with the manufacturer's specification, including power outlet, power consumption and clearance requirements and the application laws

13. All Customer's equipment must be put within TSC's licensed area and they must be either rack-mounted or be put in TSC's provided fixed partitions. None of Customer's equipment is allowed to stack or rest on the equipment of any other customer

14. All of the cables and wiring in the customer's licensed area must be neatly labeled, wrapped and tied together (if a customer fails to do so, TSC may opt to neatly wrap and tie such wires and cables, and TSC may charge the customer for performing such service)

Electrical Power

1. The Customer should only use those power sockets as assigned by TSC.

2. It is the Customer's sole responsibility to ensure the power provided as agree by the TSC is sufficient to power the devices for regular use.

3. TSC may independently inspect the power configuration of any cabinet within customer's licensed space, at any time.

4. TSC may direct Customer.
   a. To alter the power configuration of customer's equipment,
   b. To disconnect power supply to the customer's equipment or,
   c. Require customer to remove any equipment, if TSC considers that the continued operation of Customer's equipment;

i. Causes a threat to safety to the operations of TSC DATA CENTRE or property.
ii. Unreasonably interferes with the operation of TSC, any other customer or any entity utilizing any portion of the DATA CENTRE.
iii. in not installed in accordance with the standard industry practice and/or
iv. is consuming or has consumed excessive power.
v. TSC reserves the right to disconnect any unauthorized power connection made by customers.

Remarks

If Customer breaches any of the terms mentioned in this policy, TSC reserves the rights to suspend or to disconnect the services partly or wholly, or restrict Customer or it Sanctioned users from accessing the licensed area without incurring any liabilities or obligations.

TSC may change this Policy from time to time and the revised Policy shall be posted at TSC homepage at http://helpdesk.lakeheadu.ca/policies-and-procedures.html. The Customer is required to review TSC's website regularly to keep itself informed of the most current version of this policy at all times.