ACCESS CONTROL PROCEDURES

PURPOSE
1. The purpose of these Procedures is to outline the process for authorizing, monitoring and controlling the Access to all University Facilities.

DEFINITIONS
2. For the purposes of these Procedures the following definitions apply:
   
   “Access” means the issue of a key, Access Card or biometric Access to a University Facility.
   
   “Access Card” means a specialized ID card that is programmed for use with an electronic locking system.
   
   “Authorized User” means any individual who has been issued a key, Access Card, or biometric Access to a University Facility.
   
   “Biometric Reader” means a specialized electronic reader that is programmed that scans ones finger impression for use with an electronic locking system.
   
   “Designated Authority” means the person in each Faculty or Department who has been designated to establish, authorize and maintain Access control measures for University Facilities within their respective area(s).
   
   “Electronic Access Control” means an electronic locking system that is activated by an Access Card or Biometric Reader.
   
   “Exterior Building Key” means a key or Access Card that operates the exterior door locks for a Building.
   
   “Grand Master Key” means a key or Access Card that operates interior and exterior locks for multiple buildings.
   
   “Master Key” means a key or Access Card that operates all locks within a single building.
   
   “Secured Key” means a Sub-Master Key, Operational Key or Access Card to a University Facility that has restricted Access.
   
   “Sub-Master Key” means a key or Access Card that operates one group of locks within a building (e.g. a suite of doors or all doors on an entire floor).
   
   “Operational Key” means a key or Access Card that operates a single lock and/or set of locks that are keyed alike.
“University Facilities” means all locations and spaces owned and/or leased by University of Ontario Institute of Technology (UOIT) for the purposes of carrying out University activities.

PROCEDURES

3. General

3.1. Access to any University Facility will only be issued to individuals who meet the requisite knowledge, training and certification for the respective Facility.

3.2. The Director of the Office of Campus Infrastructure and Sustainability (OCIS) or designate is responsible for:
   a) Making recommendations for the establishment, review and revision of University-wide policies and Procedures related to Access control measures for all University Facilities.
   b) Ensuring that Access control measures are compliant with all applicable municipal, provincial and federal laws.
   c) Authorizing all requests for keys, Access Cards and Biometric Access.
   d) Collaborating with Designated Authorities to ensure that adequate Access control measures are established and maintained for the University Facilities they are responsible for.
   e) Authorizing the installation, management and maintenance of locks and Electronic Access Control systems.
   f) Establishing and monitoring a process for the regular audit of Access control measures for all University Facilities.

3.3. The Designated Authority is responsible for:
   a) Collaborating with the Director of OCIS and other stakeholders to establish and manage Access control measures for their area(s) of responsibility.
   b) Authorizing all requests for keys, Access Cards and Biometric Access prior to the submission to OCIS, issuing keys within the faculty or department, reporting lost keys to OCIS, and conducting departmental Access control audits.
   c) Ensuring that all individuals for whom they authorize Access are informed of and are in compliance with applicable University policies and Procedures regarding their Access.

3.4. Office of Campus Safety is responsible for:
   a) Periodically patrolling the University Facilities and identifying any suspected deficiencies or activities that threaten success of the Access Control policy objectives.

3.5. Staff and Students are responsible for:
   Compliance with these Procedures supporting the UOIT Building Access Control Policy. Specifically:
   a) Entering only the areas for which they have been granted Access.
b) Entering hazardous areas only when competent to do so and authorized to do so or under the direct supervision of someone who is authorized to do so.

c) Reporting non-compliance to their Faculty Supervisor/Manager.

d) Respecting the direction of Office of Campus Safety.

e) Returning keys/cards when the need / purpose for which they have been issued is no longer valid.

f) Reporting lost keys or Access Cards to the Designated Authority for their department.

4. **Keying System**

4.1. OCIS implements systems that will ensure security and reasonable convenience to departments occupying buildings or Facilities.

5. **Fabrication**

5.1. Except for work performed by on-site contractors or contracting service providers under the direction of the office of OCIS, the fabrication of keys and all lock work for campus facilities is delivered for OCIS by Durham College Facilities Maintenance (DCFM). Locks may not be changed by external locksmiths without the express permission of the Director, OCIS.

5.2. UOIT keys may not be duplicated except by DCFM or an agent authorized by the Director, OCIS.

6. **Requesting Access**

6.1. Access may be requested on a continuing or temporary basis depending on the stated need.

6.2. Requests for keys, Access Cards, including new Cards or the programming of existing cards, and Biometric Access must be submitted using the appropriate Access Request Form.

6.3. **Key Access Request**

   a) Individuals requiring Access to a key controlled building/room must submit to OCIS a completed Key Request Form approved by the appropriate approval authority. Approval authorities are outlined in Schedule A of these Procedures. Requests are valid for 30 days.

   b) Requests signed by the Designated Authority may be submitted by hardcopy or electronic copy. The Designated Authority should retain a signed copy for their records. OCIS will forward all approved requests to DCFM with a return copy to the requestor.

   c) Under normal circumstances keys will be ready for pick up within 5 business days after the key request has been received by DCFM. An email will be sent indicating the key is ready for pick-up. Individuals must present their UOIT Identification when picking up their key(s).

   d) Only one key will be issued per person for a specific lock. Requests for a replacement key or additional keys must include supporting rationale for the replacement or additional keys.
e) Faculties requesting limited or restricted Access to their spaces must contact the Director, OCIS for assistance. The Director, OCIS will evaluate the request and may seek the assistance of the Director, Campus Safety, Occupational Health & Safety Officer (OHSO), and the Radiation Safety Officer (RSO) in arriving at a decision. During the evaluation process, the potential risks associated with delayed or restricted Access in an emergency situation will be considered. Parties requesting limited Access or restriction to spaces must have a plan in place to ensure that a Designated Authority is available on a 24 hour basis in case a situation requiring urgent Access should arise.

6.4. Access Card Request

a) Individuals requiring Access to an electronically controlled building/room must submit a completed Access Card Form to OCIS approved by the appropriate approval authority. Approval authorities are outlined in Schedule A of these Procedures.

b) If the individual requesting the Access Card does not have a UOIT identification card with chip reader on the front of the card, then a card will need to be obtained first from photo ID at photoid@dc-uoit.ca.

7. Discontinuing Access

7.1. When an Individual no longer requires Access to a UOIT room or building, it is the responsibility of the Designated Authority to notify OCIS to ensure that Access Card Access is deactivated and that the individual returns all key(s) issued.

7.2. Keys are to be returned to DCFM to ensure their record is cleared. A copy of the Access record will be sent to the Designated Authority for their records.

8. Service Access

8.1. The Designated Authority for a given area must provide their approval before Access can be provided to perform any routine or scheduled maintenance, inspection, construction or service of any University Facility.

a) The Designated Authority is responsible for coordinating with the users of the University Facility, OCIS or other applicable department or service provider for ensuring that timely and appropriate Access and can be provided.

b) Keys, Access Cards and Biometric Access may not be issued to a service provider without the approval of the Designated Authority.

c) Individuals and service providers who have pre-existing Access (i.e. Master Key authorization) may not Access a University Facility laboratory without a completed UOIT Maintenance/Repair/Project Entry Permit and the prior approval and scheduling with the Designated Authority.

9. Restricted Access

9.1. Access to University Facilities which are deemed hazardous and/or have special security requirements must have the approval of the Designated Authority, as well as the Principal Investigator, Biosafety and Radiation Safety Officer (BRSO), and/or Health and Safety Officer as applicable before Access will be approved by OCIS. Examples of restricted University Facilities include but are not limited to: electrical switch vaults, boiler plants,
biological teaching or research labs with Biohazard Level 2 designation or higher, animal 
labs with the ASL-1 Level designation or higher, Radiation Level 2 rooms and labs, or labs 
designated by the BRSO as having other specific hazards.

9.2. Access to University Facilities with radiation level ratings require the submission of an 
authorization form for entry to radiation restricted level areas in addition to the 
Procedures set out above for requesting a key or Access Card. Access to these Facilities 
requires the approval of the BRSO.

10. Emergency Access

10.1. In the event of an emergency, Access control will be the responsibility of the Emergency 
Management Response Team (EMRT) established under the Emergency Preparedness Plan 
or the individual having jurisdiction for the response to the event.

10.2. Reasonable efforts will be made to communicate with the Designated Authority once the 
immediate threat has been resolved.

11. Lost Keys /Access Cards

11.1. Individuals possessing keys and Access Cards to University Facilities are responsible for 
such keys and Access Cards. UOIT has the authority to charge individuals for the cost of key 
and Access Card replacement.

11.2. If an individual loses a key or Access Card, or it is stolen, the individual must report this 
immediately to OCIS and also notify the Designated Authority. A replacement key or 
Access Card may be issued through completion of the appropriate Access Request Form.

11.3. If the loss of Grand Master, Master, Sub-Master, Secure key(s) or an Access Card with the 
same Access privileges as the previously noted key level is discovered, the employee must 
report the event directly to Campus Security immediately (ext. 2400).

RELEVANT LEGISLATION

12. This section intentionally left blank.

RELATED POLICIES, PROCEDURES & DOCUMENTS

13. Access Control Policy

   Key Request Form

   Access Card Request Form

   Emergency Preparedness Plan

   Authorization For Entry To Radiation Level 2 Restricted Area Form

   Maintenance/Repair/Project Entry Permit
<table>
<thead>
<tr>
<th>Access Level</th>
<th>AUTHORIZED USERS*</th>
<th>Approval Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>• Individual users of the University Facility (e.g. office, teaching or research lab, classroom)</td>
<td>Authorized by: • Designated Authority and • Director, OCIS</td>
</tr>
<tr>
<td>Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exterior Building</td>
<td>• Building occupant</td>
<td></td>
</tr>
<tr>
<td>Sub-Master Access</td>
<td>• Vice-Presidents, Deans, Managers, Directors and other authorized administrators for areas under their control • Signed-Out on a daily basis to Facilities staff, maintenance personnel and ITS staff</td>
<td>Authorized by: • Designated Authority, • Vice-President/Dean, • Vice-President, Human Resources and Services and • Director, OCIS</td>
</tr>
<tr>
<td>Master Access</td>
<td>• Vice-Presidents, Deans, Managers, Directors and other authorized administrators for areas under their control • Signed-Out on a daily basis to Facilities staff, maintenance personnel and ITS staff</td>
<td></td>
</tr>
<tr>
<td>Grand Master</td>
<td>Not Provided</td>
<td></td>
</tr>
<tr>
<td>Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secured Access</td>
<td>• Individual users of the University Facility as required by their position</td>
<td>Authorized by: • Designated Authority, • Vice-President, Human Resources and Services and • Director, OCIS Depending on the University Facility and restriction, authorization may also be required by: • Principal Investigator and • Biosafety and Radiation Officer or, depending on nature of secured Access, Health and Safety Officer</td>
</tr>
</tbody>
</table>