1.0 Purpose

The purpose of this Policy is to set out the principles that apply when granting and managing building and facility access on the University of Guelph’s main campus. The processes which support this Policy are further outlined in applicable standard operating procedures (SOPs) as referenced above. This Policy
2.0 Scope
This Policy applies to all facilities and buildings located on the University of Guelph’s main campus and applies to all Campus Users of these facilities. This policy does not include those facilities that are owned, operated, or leased on lands outside of the main campus property with the exception of Family Housing communities operated by Student Housing Services.

3.0 Preamble
The University of Guelph is committed to providing operational and administrative processes that support the safety and security of University facilities and users. Managing access to University facilities must take into consideration the responsibility to uphold the privacy and protection of those who work and reside on campus. In order to safeguard community members, campus facilities and the physical assets of the University, this Policy and applicable procedures have been developed to outline specific expectations and standards.

The University has determined that electronic access and control technologies provide superior protection and flexibility for managing building access control. As such, the University has committed to the use of electronic access systems, as appropriate, and as determined by Physical Resources, for i) all new construction, ii) major renovations and iii) retrofits to existing buildings on a priority basis.

4.0 Definitions
4.1 Access Security Level:
Refers to a building’s security designation determined by the AVP Physical Resources and the Director Campus Community Police (i.e. Level 1 (Standard), Level 2 (Medium), Level 3 (Maximum)).

4.2 Building Access Control:
Refers to how the security and protection of a building or facility is managed.

4.3 Campus User:
Refers to individuals who are authorized for key access to a building, room or facility on the University of Guelph’s main campus.

4.4 Designated Authority:
Refers to the individual that has been authorized and designated to administer key approval for their department, unit or division.

4.5 Hardware Key:
Refers to metal hardware that is used to open a lock mechanism for a door, building or storage area.

4.6 Electronic Access:
Refers to an electronic card access system (card reader) that controls locking mechanism on doors, buildings and facilities.

4.7 Key:
Refers to a hardware key or other device (i.e. fob, coded University ID) that grants access to a particular area, room or building.

5.0 Policy

5.1 Authority
5.1.1 Under authority of the VP Finance, Administration and Risk and the direction of the Associate Vice President, Physical Resources, the division of Physical Resources is responsible for the overall physical operation of building access for facilities on the University of Guelph’s main campus. This includes but is not limited to, the installation, administration, maintenance, repair, and implementation of building access (i.e. door hardware, electronic access).

5.1.2 In rare circumstances, the VP Finance, Administration and Risk may approve direct responsibilities for the operation of building access within a specific department (e.g. Student Housing Services) or to a Designated Authority. This may include but is not limited to managing of key requests, modifications to electronic access, and key assignments.

5.1.3 The Associate Vice President, Physical Resources and the Director Campus Community Police (or their designate) are responsible for determining the Access Security Level for all main campus buildings or facilities as per 5.2.2 and have ultimate discretion over individual user authorization.

5.1.4 The structure of authorization levels of key access (e.g. pass key, sub-master, master etc.) outlined in Appendix A, are subject to the approval of the Associate Vice-President, Physical Resources.

5.1.5 Campus Community Police has the ultimate authority to override a building access control as part of the University’s Emergency Management Plan for the overall safety and security of campus community.

5.1.6 All keys (i.e. door key, ID card, fobs) issued for a campus building or facility are subject to this Policy, and are the property of the University.

5.2 Safety and Security
5.2.1 The provision of safety, security, and privacy are paramount in consideration of building access. Campus Users shall be granted building access based on the lowest level required to fulfill their essential job duties or service provider duties.

5.2.2 The Designated Authority is responsible for authorizing Campus Users and defining the appropriate...
access level. Additional authorization is required for higher levels of access as per Appendix A.

5.2.3 Physical Resources will only issue building access to individuals who have been authorized by the appropriate Designated Authority.

5.2.4 Each building or specific area will be designated with an Access Security Level to safeguard the property, materials, and assets. Access Security Levels are also determined by the stakeholder needs (e.g. hours of operation, need for public access etc.) and in consideration of any potential or perceived risk. Access Security Levels for building access are classified as the following:

i) Level 1 (Standard): Buildings or specific area that have no access restrictions during normal business hours and where perimeter protection is the only requirement. Level 1 is where vulnerability of common area assets are minimal, asset protection systems are present, and incidents of loss are infrequent.

ii) Level 2 (Medium): Buildings or specific area that have access restrictions during normal business hours (i.e. 8:30am to 4:30pm) or interior areas that require electronic access. Level 2 is where there is a moderate risk to property, vulnerable assets, and/or incidents of loss or damage is frequent.

iii) Level 3 (Maximum): Buildings or specific area that have 24/7 perimeter access control. Maximum Security level is where there is a significant risk or vulnerability to high value assets/materials and/or health, safety, or security risks to users.

5.2.5 Keys shall not be sent through University mail and must be picked up in person from the Physical Resources Lock Shop.

5.2.6 At the request of the University, a Campus User may be required to submit a Criminal Background or Vulnerable Sector Check for the security of the campus community.

5.2.8 The Director Campus Community Police, Emergency Management and Fire Safety is responsible for ensuring external emergency responders (e.g. Guelph Police, Guelph fire etc.) have the appropriate building access in accordance with the Emergency Management Plan.

5.2.9 To ensure emergency access, no room or area on the main campus shall be secured by means other than locking devices approved by the Director, Maintenance & Energy Services. No lock shall be taken off the University’s master keying system unless approved in rare circumstances by the Director, Maintenance & Energy Services and the Director, Campus Community Police, Emergency Management & Fire Safety.

5.3 Campus User Responsibilities
Failure of a Campus User to carry out the responsibilities below may result in loss of privileges, penalty (e.g. fine), disciplinary action and/or charges through the Campus Community Police.
5.3.1 Campus Users shall use and care for key(s) in a responsible manner. Unauthorized possession or use of a University key is prohibited.

5.3.2 Copying, lending, or altering a University key is strictly prohibited.

5.3.3 Campus Users are prohibited from taking Sub Masters, Masters, and Grand Masters hardware keys off main campus property. Only pass level keys and electronic access ID cards, which are required to enter a workplace, may be taken home.

5.3.4 Campus Users who are authorized for Sub Masters level keys and greater, must ensure they are stored in a secure manner within the Campus User’s workplace.

5.3.5 Campus Users who are granted building access are only authorized for their designated areas and times.

5.3.6 Campus Users must report the loss or theft of any key(s) to their immediate supervisor and Campus Community Police as soon as possible.

5.3.7 Defective or broken hardware keys shall be reported and returned to the Physical Resources, Lock Shop. Defective electronic access keys shall be reported to Electronic Access at eaccess@pr.uoguelph.ca.

5.3.8 If affiliation or employment status changes with the University, Campus Users shall surrender all hardware keys to their supervisor or Designated Authority, and the Designated Authority must also update eaccess@pr.uoguelph.ca with any electronic access changes. The University retains University ID cards where the individual is no longer employed with the University, unless otherwise approved by the Dean/Director/Chair. Physical Resources may also alter or remove access if notified by Human Resources.

5.4 Responsibilities of Designated Authority and/or Department

Failure to uphold Designated Authority/Department Responsibilities may result in loss of privileges, penalty (e.g. fine), or other action from the AVP Physical Resources.

5.4.1 Designated Authorities and their departments are responsible for keeping accurate records of key Access Levels, key assignments and Campus Users.

5.4.2 At the request of Physical Resources, departments and/or Designated Authority shall perform an audit of keys, records, and/or Campus Users.

5.4.3 Departments are responsible for any costs and or penalties associated with, but not limited to, key loss, theft, replacement, repair, or rekeying.

5.4.4 All department keys (i.e. hardware key and fobs) which have become obsolete shall be returned to the Physical Resources Lock Shop.
5.4.5 Advise Physical Resource’s Lock Shop and/or Electronic Access immediately, to avoid delays in granting building access, if there is a change in Designated Authority.

5.4.6 Arrange and administer all access to academic or administrative buildings or areas to students as needed.

5.4.7 Designated Authorities are responsible for approving secure storage systems or methods for their Campus Users’ keys. Physical Resources may be consulted for recommendations on secure storage systems or methods.

5.5 Contractors and External Services Providers
Building access requests (i.e. keys and electronic access) for individuals not affiliated with the University, including but not limited to, contractors and delivery agents are managed by Physical Resources, unless otherwise approved Physical Resources. For more information please see Building Access Procedures for Contractors.

To receive this document in an alternative format please email wo@pr.uoguelph.ca.
Appendix A: Building Access Control Authorization

The following chart outlines the types of keys used for main campus buildings/facilities and the authorization required for Campus Users for key possession.

<table>
<thead>
<tr>
<th>Building Access Control Authorization Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Key</td>
</tr>
<tr>
<td>Pass Key</td>
</tr>
<tr>
<td>Building Sub Master</td>
</tr>
<tr>
<td>Special Master</td>
</tr>
<tr>
<td>Building Master</td>
</tr>
<tr>
<td>Grand Masters</td>
</tr>
</tbody>
</table>

- Additional authorized users, controls, or authorizations may apply for keys which access student accommodations.
- Contractors or external providers must follow additional procedures as per Building Access Procedures for External Providers and Contractors.
- Hardware keys are issued by Physical Resources Lock Shop after approval from Designated Authority. Electronic Access granted by Physical Resources (Electronic Access Group) after approval from Designated Authority.
- Structure of Building Access Control Authorization Levels is approved by the AVP Physical Resources.