Security, Access Management and Key Control Policy and Procedures

1.1 Policy

1.1.1 The goal of the Vice President, Business Affairs and Facilities and Services is to provide a safe, comfortable, secure learning environment for the University while minimizing occurrences of theft or damage to equipment, furnishings and other property. Security of the building and building access management is the responsibility of Faculties, Divisions and Departments that have been assigned control over space. The University of Toronto operates a centralized key and electronic access management system to ensure consistency and effectiveness in an efficient and economical manner. Designated Authorities (DA) are assigned for faculties and administrative divisions having control over doors and locks. Designated Authorities will request keys and credentials through software or on forms approved for the purpose. The requesting designated authority is responsible for the cost of issuing keys and credentials.

1.1.2 The University has more than 130 buildings, 100,000 doors and countless windows. Providing physical security in a large physical plant requires standardization on a range of products and protocols. At the same time, Faculties, Divisions, and Departments must be supported in managing space assigned for their use.

1.1.3 Facilities and Services will assist Faculties, Divisions, and Departments in establishing an ongoing Key Control System and Access Management System. Each Faculty, Division and Department will appoint an Access Management and Key Coordinator, known as the Designated Authority whose responsibility will be to authorize persons to have access to locked space through the use of a key, a numeric combination or an electronic credential.

1.1.4 The Manager, Police Services will be responsible for ensuring the administration of and compliance with this policy. Police Services are the only authorized providers of access control systems and credentials for use with them.

1.1.5 The Lock Shop is the only authorized provider of keys on the campus. Keys may only be created with the approval of the appropriate designated authorities through the Property Manager. Master keys may only be issued with the approval of the Manager, Police Services. The Lockshop will maintain a record of every key provided to a designated authority for distribution within their faculty, division or department. The Designated Authority will record who every key is issued to and its return. Returned keys may be reissued or returned to the Lockshop for destruction.

1.2 Standards

1.2.1 Facilities and Services, on behalf of the University, have established standards for locks, keys, doors, windows, electronic access management systems and credentials. All new construction and renovations to existing space will conform to the standards established in this policy. Standards are valid on the date of their publication and remain valid until modified by the University or rescinded. Standards are found at the Facilities and Services website at www.designstandards.utoronto.ca.

1.2.2 Contractors are responsible to ensure they are using the latest standard when supplying and installing devices. Property and Project Managers will ensure compliance with this policy when requesting work to be done.

1.3 Definitions

In this policy, the term:

1.3.1 **Credential** refers to a device that activates an electronic reader which in turn causes the system to activate a mechanical device or disengage a lock, permitting access to an area that is otherwise locked. Credentials are commonly referred to as access cards, card keys or access key fobs.

1.3.2 **Card Management System** refers to the software and hardware used to manage request and issuance of credentials to authorized persons.

1.3.3 **Key** refers to a device that is inserted into a locking mechanism to mechanically cause the lock to disengage, permitting access to an area that is otherwise locked.

1.3.4 **Key Management System** refers to software and hardware used to manage request and issuance of keys to authorized persons.

1.3.5 **Numeric combination** refers to a sequence of numbers depressed or dialed that disengages a lock, permitting access to an area that is otherwise locked.

1.3.6 **Biometric** refers to an electronic representation of a physical attribute of the person such as an iris, a hand, a finger or facial features

1.3.7 **Designated Authority** is the person appointed by the head of a faculty, division or department to be responsible for permitting access to space controlled by the faculty, division or department.

2 Access Management

2.1 Responsibility

2.1.1 The Designated Authority for each Faculty, Division or Department is responsible for requesting keys, credentials and changes to locks. The Designated Authority for each Faculty, Division or Department is responsible for the issuance and control of all keys to the related Faculty, Division or Department. The Faculty, Division or Department is responsible for the cost of replacing lost, stolen, broken or worn keys.

2.1.2 Systems provided for requesting and issuing access credentials and keys will be used by the requesting designated authority when provided.

2.1.3 Facilities and Services is responsible for:

2.1.3.1 Issuing keys and credentials as authorized by the Designated Authority;
2.1.3.2 Ensuring that requests are signed by a valid Designated Authority;
2.1.3.3 Making changes within a reasonable time frame;
2.1.3.4 The operation, maintenance, repair and replacement of door lock cylinders and lock sets, controllers, readers and other devices that form the access control system.
2.1.3.5 Managing the key locking and access control systems and fairly apportioning costs to the Faculty, Division or Department responsible for the space.

2.1.4 A Faculty, Division or Department requesting:

2.1.4.1 a change to the key system such as re-keying and replacing lock sets and cylinders is responsible for the cost of the change.
2.1.4.2 installation of a security system other than lock and key, including electronic, mechanical combination and card or other credential access locking systems
2.1.4.3 is responsible for the cost to install, maintain, repair and replace the system.

2.2 Compliance with Standard

2.2.1 No campus area may be secured except by a locking device authorized by Facilities and Services. Where an electronic lock or access control system is installed, a security keyed lock shall also be installed as a manual override in the event of failure or emergency. To ensure controlled access for emergency services, all cylinders will be keyed to the building master. Under special and limited circumstances, with the authorization of the Manager, Police Services, a cylinder may be taken off the building master but it will be keyed to the Fire Master.

2.2.2 Keys or credentials that permit access to space owned, operated or leased by the University may be issued to individuals affiliated with the University. All keys and credentials are the property of the University of Toronto and will be surrendered on the demand of a Designated Authority, a University of Toronto Special Constable or a supervisor.

2.2.3 Upon receipt of a key or credential, the holder agrees:

2.2.3.1 to the proper use and care of the key or credential;
2.2.3.2 to not loan, duplicate or use it in any unauthorized manner;
2.2.3.3 to pay the established fee for replacement if lost or damaged,
2.2.3.4 to return or surrender it to the issuing authority, or designate, upon demand.

2.3 Designated Authority

2.3.1 Each Faculty, Division or Department must appoint a Designated Authority who will be responsible for approving and authorizing all key, credential access requests, and lock changes for the Faculty, Division or Department. The "Designated Authority Form" (see appendix I) must be used to initiate or change the Designated Authority. The Manager, Police Services will request an update of Designated Authorities on an annual basis.

2.3.2 A request for issuance of a key or credential must be approved and authorized by the appropriate Designated Authority. All requests will be reviewed by Facilities and Services and will not be acted upon if not properly authorized.

2.3.3 As a general principle, issuance of master keys or credentials will be limited to those persons:

2.3.3.1 Requiring access to space as part of their responsibility and
2.3.3.2 If the issuance of multiple sub-masters would be impractical.

2.3.4 All requests to cut building master keys must be approved by the appropriate Vice- President, Principal or Dean and the Manager, Police Services. For multi-Faculty, Division or Department buildings, all Designated Authorities must sign and agree to any building master key being issued.

2.3.5 When electronic, networked access control systems are installed in any building, master over-ride keys for exterior doors will not be cut or issued to anyone other than a member of the University Police Service, Fire Prevention Service or Locksmith for use during the course of their duties.

2.3.6 All approvals must be as per appendix II.

2.4 UTorId

2.4.1 The University has established a database known as UTorId to manage access to computers and other systems. Data is drawn from a number of sources including student and personnel records. The access control system will access data from the UTorAuthId and assign access based on an agreed plan provided by the designated authority. Credential authorizations will be modified or disabled when status changes.

2.4.2 Data obtained for the purpose of managing the access control system will be used for no other purpose and will be maintained in a confidential file. Access to the file will be restricted to those persons authorized to administer the system.

2.5 Issuance of Keys and Credentials

2.5.1 A Service Order Form (see appendix III) must be completed and signed by the Designated Authority for all key or credential requests. Forms can be obtained from the Property Managers or by calling 416-978-3000.

2.5.2 The completed Service Order Form must be forwarded or faxed (416-978-3001) to Property Management at 215 Huron Street.

2.5.3 Key Management Software will be used when provided for the purpose of automating the request for and issuance of keys to authorized persons.

2.6 Distribution of Keys and Credentials

2.6.1 Keys and credentials will be returned to the designated authority for distribution. Upon completing the order, Property Management will notify the Designated Authority or the Contact Person that the key(s) have been made or credentials prepared. Upon notification, the Designated Authority or the Contact Person will arrange to pick up the key or credentials from Police Services, 21 Sussex Avenue or make alternative arrangements with the Property Manager.

2.6.2 In the event that a credential has been lost and the identity of the person has been confirmed in the system, Campus police may replace the credential at the expense of the individual or the Department, Faculty or Division as determined by the Designated Authority.

2.6.3 Each Designated Authority is responsible for keeping records of keys and credentials issued to and returned by Faculty, Staff and Students. Credentials and keys may be reassigned by Campus Police. All changes in assignment of the credential or key must be recorded at the police services office by completing the appropriate notification form.

2.6.4 Key and Credential Return

2.6.5 It is the responsibility of the immediate supervisor to ensure that keys and credentials issued to faculty, staff and students and authorized holders, are returned to the Designated Authority or Contact Person when it is no longer appropriate for the person to have keys or credentials. The Designated Authority will return the building master keys and credentials to the Manager, Police Services. Keys and credentials should be recovered if the following occur:

2.6.5.1 Transfer to another department, position or building.
2.6.5.2 Termination, resignation or retirement.
2.6.5.3 Completion of the term of employment or the temporary record of issue.
2.6.5.4 Completion of the Academic term or the temporary issue period as specified by the Designated Authority.
2.6.5.5 Credentials may be retained by returning students but will be deactivated during the summer unless required. Permission to keep a card active must be given by the designated authority on the appropriate form.

2.7 Padlocks, Peripheral and Personal Locks

2.7.1 All padlocks to doors or gates affecting University property must be compatible with the authorized key control system. All keys to these locks will be controlled in accordance with prescribed policy.

2.7.2 Key(s) to filing cabinets, desks, and personal lockers etc. will remain the responsibility of the person in charge of the area.

2.8 Lost or Stolen Keys or Credentials

2.8.1 All lost or stolen building keys or credentials must be reported to the University of Toronto Police.

2.8.2 If a building master key is lost or stolen, Facilities and Services will communicate this to the relevant Designated Authority and a mutual decision based on the risk involved will govern the action to be taken. If the action results in a re-keying operation then the costs for this action will be charged to the party responsible for the loss of the key.

2.9 Key or Credential Replacement

2.9.1 A new Job Request Form must be submitted for key replacement. Damaged and broken master keys, including broken pieces, must be returned or accounted for before a replacement may be issued.

2.9.2 Cylinder replacement or pin combination change as a result of lost or stolen key will be in accordance with the charges authorized in appendix V.

2.9.3 In the event that a credential is lost, stolen, damaged or ceases to function, Campus police may reissue the device once they are satisfied of the identity of the holder. The cost of replacement will be borne by the appropriate faculty, department or division. No charge will be made for replacing defective devices caused by manufacturing defects.

2.10 Repair of Locks, Keys, or Door Hardware

2.10.1 The University of Toronto has contracts with suppliers for high security keying and access control systems. These contracts impose a number of restrictions to maintain the integrity of the systems.

2.10.2 Only Facilities and Services Lock Shop personnel are authorized to re-key, repair and relocate University cylinders. Only an authorized technician may repair any portion of the access control system.

2.10.3 All repairs or additions to any locking device, card reader, request to exit, electric strike or electric lock, controller, key or door hardware installed by the University shall be managed by Facilities and Services and documented with a numbered work order. Work orders are managed by the Property Manager who will ensure compliance with this policy.

2.11 Facilities and Services Staff

2.11.1 Permanent assignment of keys or credentials to Facilities and Services staff shall be made only in cases of demonstrated need for operating safety and security reasons. Approval for this assignment must be given by the Director of the appropriate Facilities and Services Division. A record of all persons who hold such key(s) will be maintained by the Manager, Police Services.

2.11.2 The remainder of key and credentials shall be assigned daily on a temporary basis to allow access to the work area assigned (if work area is secured). The keys and credentials shall be returned at the end of each work shift and verified by their supervisor.

2.12 Key Issuance to Outside Contractors

2.12.1 Contractors requiring keys and credentials for access to campus facilities must obtain the approval of the Project Manager or Property Manager and, when appropriate, the Manager, Police Services the Director of Building Services and Grounds or the Director of Utilities.

2.12.2 Every person employed or authorized by a contractor to sign out keys will complete a personal history form which will be filed at Campus Police and retained for a minimum of one year after completion of the project.

2.12.3 Police will pick up all prepared keys during the business week prior to 4:00 p.m. at the Lock Shop. If keys or credentials are needed after normal hours, the Facilities and Services person supervising the contract will deliver the keys and credentials to the police office.

2.12.4 Keys and credentials will be signed out by an appropriately identified contractor representative for one shift and signed back in at end of the shift but no less than once per day. An authorization to recover costs for re-keying in accordance with Appendix V associated to lost or stolen keys must be signed by the contractor authorizing the University to deduct funds from contract fees if the key is lost or stolen or has not been returned to Campus Police.

3 Electronic Access Management, Video Surveillance and Burglar Alarm Systems

3.1 The use of video surveillance will be governed by the guidelines of the Privacy Commissioner, Province of Ontario. The Manager, Police Services must be consulted and approve the use of surveillance for any purpose on Campus.

3.2 Increasing demand for electronic door access systems promotes the need for standardization of hardware, process and control of door access, video surveillance systems and burglar alarm installations on Campus. The University has established a central station for monitoring network dial-in alarm systems. Standards are found at www.designstandards.utoronto.ca.

3.3 Manager, Fire Prevention Services is the designated fire control manager for the University of Toronto, St. George Campus. In all matters of fire prevention and detection, he/she will be consulted and will develop the appropriate hardware and software solutions.

3.4 The Manager, Police Services, St. George Campus it the designated security manager for the University of Toronto. In all matters of security, including locks and keys, access control and burglar alarm systems, video surveillance and windows and doors, he/she will be consulted and will assist in developing the appropriate hardware solutions.

3.5 Prior to design of any electronic door access system, video surveillance or burglar alarm system, a Job Request Form (Appendix III) along with the proposed plans and specifications of the system and installation must be submitted to the Manager, Police Services, 21 Sussex Avenue for review and approval. Costs for response, monitoring, maintenance, repairs and replacement are the responsibility of the Faculty, Division or Department.

3.6 The use of magnetic door locks (Maglocks) will generally NOT be permitted. Only under exceptional circumstances and with the approval of the Manager, Police Services and the Manager, Fire Prevention, will any deviations be permitted.

3.7 All doors having credential access reader or combination control must have a key override. In the event of a power failure, with the exception of Maglocks, all electronically operated locking devices must fail in the locked position. Where Maglocks are used, panic hardware must also be installed. Emergency egress will be maintained but access will be with the use of a key.

4 Procedure for Security System Planning

4.1 New Construction

The process for developing a security system option for new construction is as follows:

4.1.1 Architectural design completed.

4.1.2 Architect, User Representative and Project Manager consult Campus Police with drawings, preliminary options developed.

4.1.3 Fire Prevention, Campus Police, User Representative and Project Manager consult with users. Architect may attend if requested. Based on building use and work flow factors, a final security plan is developed which follows both the Key and Access Control Policy and the Security System Standards.

4.1.4 Project Manager has electrical and systems developed based on plan and hardware options.

4.1.5 Construction completed, system accepted and commissioned by Campus Police.

4.2 Renovation or Security Audit Implementation

The process for developing a security system option for renovation or as the result of a security audit is as follows:

4.2.1 Design or security audit competed.

4.2.2 Property Manager, designer and User Representative consult with Campus Police with design or floor plans; preliminary options developed.

4.2.3 Fire Prevention, Campus Police, Property Manager, designer and User Representative consult with users. Based on building use and work flow factors, a final security plan is developed which follows both the Key and Access Control Policy and the Security System Standards.

4.2.4 Project Manager has electrical and systems design developed based on plan and hardware options. Tenders work and supervises completion.

4.2.5 Construction completed, system accepted and commissioned by Campus Police.

4.3 System On-going costs

4.3.1 After acceptance by Campus Police, the faculty or administrative division which controls the space will be responsible for operating costs.

4.3.2 Facilities and Services will apportion operating costs and maintenance as part of the fabric charges for the building.

4.4 Additional Costs

4.4.1 Design standards indicate that suppliers will not include costing for computers and servers to manage the security or video systems. The University will purchase, through its authorized suppliers, computers and servers. Systems standard architecture is based on Dell servers and workstations. As part of the Campus Police design process, the size and functionality of the computers will be determined.

4.4.2 The University has installed a separate network to manage its security system. As part of the project, CNS will provide the necessary connectivity for the system. Property and Project managers will consult CNS at the earliest opportunity to develop plans and costing for connectivity.

4.4.3 As part of the project cost, Property and Project Managers will purchase and supply to campus police the necessary computers and network appliances for access to the system.

4.4.4 Costs are recovered from users of the system and are determined by actual experience of administering the system. As costs increase or decrease, the result will be passed on to users of the system.