ADMINISTRATIVE DIRECTIVE

Category: Accessibility and Inclusion

Key and Access Card Control

Directive Number: ANI-110
Approved by: CLT
Administered by: Public Works & Engineering, Security Services
Effective Date: December 17, 2020

1. Background

The City of Brampton recognizes the need to balance an individual's right to protection of privacy, provide reasonable access to City of Brampton buildings for authorized use. It is the City's duty to ensure the safety and security of all City staff, contractors and non-City staff while maintaining the protection of City assets.

The Key & Access Card Control Administrative Directive and any associated programs and procedures serve to secure the City of Brampton buildings and facilities.

2. Purpose

The purpose of this Administrative Directive is to:

a) Establish the business rules for the administration of access and control to City buildings and facilities.

b) Manage the issuance of all access cards and keys for all City of Brampton authorized users.

3. Application and Scope

This Administrative Directive applies to:

a) All City of Brampton buildings and facilities with the exception of Brampton Transit and the Brampton Library.

b) All City staff, members of committees, Members of Council and their staff, and non-City staff (such as vendors, tenants, contractors, consultants and volunteers acting on behalf of the City).

c) City of Brampton facilities that lease space within the building to third party organizations, tenants will be subject to this Administrative Directive unless otherwise stated in the contract and lease agreements.

This Administrative Directive should be read in conjunction with:

- Key Delivery Standard Operating Procedure
- Keywatcher Touch Standard Operating Procedure
- Key & Access Control Program Overview; and
- Related request, replacement and authorization forms listed in section 11 of this Administrative Directive.

3.1 Exceptions

a) Access and security systems within leased space in City facilities, are solely managed by third party organizations, as such, Security Services do not manage these systems. However, during pressing circumstances, Security Services will have access to these spaces.

b) Any requests for a change or exception to this Administrative Directive shall be submitted in writing to the Manager, Security Services for review and approval. Only requests that are consistent with current applicable City of Brampton directives, policies and SOPs will be considered.

4. Outcomes

The intended outcomes of this Administrative Directive are to ensure:

4.1 City staff and assets are secured and protected;

4.2 Appropriate controls, documentation and best practices are implemented;

4.3 Clear guidelines and best practices are in place to ensure staff are demonstrating due diligence with respect to issuing, monitoring of identifications and key access to City facilities.

5. Principles

5.1 **Reasonable and Secured Access –** All issuance of security access cards and keys will be completed in a manner that balances reasonable access and security in accordance to this Administrative Directive.

5.2 **Protection of Assets –** Ensure the safety and security of staff, contractors, clients, consultants and City assets.

6. Mandatory Requirements

6.1 The City will administer access cards and hard keys to authorized staff and non-City staff, as per this Administrative Directive, supporting guidelines and procedures.

6.2 When no longer required all access cards and hard keys issued to a person must be returned to their immediate supervisor, mananger or City representative and further returned to Security Services.

6.3 The distribution, organization and safekeeping of access cards and keys are maintained by Security Services.

6.4 All security access requests must be submitted to Security Services using the most current processes.

6.5 Duplication or altering, in any way, of City of Brampton access cards and keys is prohibited.

a) Where prohibited duplication or unauthorized keys have been identifed, these shall be retained by Security Services. Security Services will also conduct an investigation.

6.6 The transfer of access cards to another person(s) is strictly prohibited and are only to be used by the person whose photo and name appears on the card.

a) This provision includes daily or temporary use access cards.

6.7 The transfer of hard keys to another person(s) is strictly prohibited and are only to be used by the person whose signature and name appears on the Hard Key Request Form.

a) This provision includes hard keys, which are signed out and returned daily for use.

6.8 Temporary users will be authorized only on the date and within the time frame provided by Security Services.

6.9 Staff and or contractors who have been issued access cards for the purposes of Daily or Temporary Use are to return items daily to Security Services, unless otherwise authorized by the manager of Security Services.

6.10 Upon separation of employment or contract termination, all issued access cards and keys must be returned to the respective supervisor or manager. Supervisors or managers must return all access cards and keys to Security Services as soon as practicable.

7. Master Keys

7.1 Master keys are not to be in the possesion of staff unless actively working, and are to be secured on site

7.2 Departments with staff working in an on-call capacity, where the use of a master key is required, will need to seek the approval from Security

Services in order to obtain a ‘on-call’ master key ring to be used for the authorized duration.

a) At the end of each on-call period, the on-call master key ring will be logged back into a key ledger by the authorized designate and signed out to the next on-call staff member.

7.3 Each staff member will not be issued their own on-call master key ring.

8. Roles and Responsibilities

8.1 Commissioner

- The Commissioner that is responsible for Security Services and/or authorized designate by the CAO can approve all grand and great grand master key requests for all city facilities governed under this Administrative Directive.

8.2 Security Services

- Maintains oversight over the issuance, activation and record keeping of all City of Brampton hard keys and access cards.
- Reviews all security requests forms in conjunction with the requester’s designated authority.
- Reviews and certifies access authorization of all individuals for whom the security access cards and hard keys is requested.
- Notifies requesters as soon as practicable once the hard key(s) and/or access cards are available.
- Maintains a secure computerized database that manages and supports key issuance records and City of Brampton Access Card programming for City of Brampton facilities.
- Develops a detailed security incident report for all lost keys and access cards. Where warranted, an internal risk assessment may be conducted by Security Services who will determine that may result in the re-keying of an area/facility.

8.3 Security Manager or designate

- Ensures the implementation of and compliance with this Administrative Directive.
- Acts as the designated authority for all security systems, installations, including locks and hard keys, access control systems, alarm systems and surveillance systems.

- Reviews all documents and stock inventory and ensures proper authorization and justification for issuance security access cards.

8.4 Key & Access Control Coordinator

- Ensures intake, issuance and retrieval of all hard keys and access cards.
- Maintains and updates all master records and documents.
- Conducts periodic audits of stock inventory and records.
- Assurance of all training, inspections and audits with key designate. Reports and tracks all discrepancies and necessary corrective actions to the Security Manager or designate.
- Conducts periodic audits of issued hard keys to verify key numbers, sequence numbers and markers against the hard key control inventory.

8.5 Department Key and Card Designated Authority

- Department Director or their authorized designate(s).
- Responsible for submitting Key and Card Access requests and changes (provides approvals for access within their department).
- Responsible for maintaining records for their department/section as designated by their director.
- Liaise with Key and Card Access Coordinator to audit and maintain records.

8.6 Access Card and Key Recipients

- All City issued cards and keys are to be treated with the same care as one would treat their personal cards and keys and are to be used only as intended.
- Responsible for the proper use of issued keys and access cards assigned to them as outlined in this Administrative Directive and in applicable terms and conditions of use.
- Ensure the immediate return of issued keys and/or access card to the appropriate person(s) when no longer needed, or upon employment or contract termination.
- Reports lost or stolen items to Security Services and to their immediate supervisor. Replacement costs for hard keys and access cards may be billed to the employee’s department.

9. Monitoring and Compliance

9.1 Inspections and Audits

Compliance will be monitored through regular inspections and audits scheduled quarterly by Security Services:

a) Process audits and inventory audits shall be conducted by the Key & Access Control Coordinator to ensure accountability of all properties and proper use.

b) Audits using established procedures will be conducted by Security Services to ensure the proper handling, accountability and accuracy.

9.2 Records

a) All documents and stock inventory shall be reviewed by the Security Manager or designate to ensure proper documentation and inventory counts.

b) The collection of records must be retained with all necessary supporting documents for the maintenance and integrity of the Key & Access Control Program in accordance with the Records Retention By-Law 272-2014, amended by By-Law 183.2015.

c) All hard keys and access cards will be documented and destroyed as stated in the supporting documents and relevant SOPs.

d) All records will be kept confidential in accordance with all related By-Laws, SOPs and best practices.

9.3 Consequences of non-compliance

a) Access cards and keys used for any non-official or unauthorized purposes may be confiscated by Security Services and the user may be subject to remedial action. All issued items remain the property of the City of Brampton and must be returned upon request by the City.

b) Evidence of any transgression in any aspect shall be brought to the attention of the Security Manager and or designate as all findings may result in an investigation.

c) Failure to comply with these provisions and procedures may be subject to corrective action.

d) All costs associated with the re-keying of an area/facility as a result of lost keys may be incurred by the department to which the keys were issued at the current rate.

e) All costs with issuing a new access card due to loss of card or deliberate alterations will be charged back to the department at the current rate.

- The following are excluded from the replacement costs;
  - Name change
  - Wear-and-Tear
  - Significant change in appearance

10. Definitions

- **Access Card** means a plastic card with a chip or magnetic strip containing encoded data that is read by tapping the card over an electronic device, used to provide access to restricted or secure areas or systems.
- **Access Control System** means a locking system that is hard-wired, consisting of hardware and software, and stores information in two places, in computer servers and in a local control panel.
- **Designated Authority** means a functional responsbility that is held by a full-time staff of the City of Brampton. Designated by the head of the department to be responsible for authorizing access to buildings, space, rooms and other interior spaces.
- **Facilities** means buildings that are leased, owned or operated by the City of Brampton.
- **Great Grand Master Key / Grand Master Key** means an enhanced access above a **Master Key** and are generally not issued to staff.
- **Hard Key** means a device inserted into a lock that allows the lock to be disengaged mechanically, thereby permitting access to a building, space, room or interior area that is otherwise locked and secured.
- **Key & Access Control Coordinator** means a functional responsibility that is held by a full-time employee of the City of Brampton within the Security Services. Assigned responsibilities include but not limited to, key control, requisition, distribution, retrieval, and record keeping of all master documents. The Key & Access Control Coordinator is also assigned responsibilities of coordinating access card requirements of all City of Brampton staff, authorized third party contractors and authorized stakeholders. This position serves as the liaison

between City of Brampton staff, authorized third party contractors and authorized stakeholders and Security Services.

- **Master Key** means a key that is designed to open several different locks.

- **Member of Council** refers to any elected or appointed official on Council, including the Mayor.

- **Non-City staff**: Persons such as vendors, tenants, contractors, consultants and volunteers acting on behalf of the City.

    - More specifically:

        - A Contractor means the party which has entered into the Contract for the purchase of Goods and/or Services awarded by the Owner under a Bid Call;

        - Consultant – An individual, corporation or other entity (including a consulting firm) that provides services in return for any form of compensation, including, but not limited to public relations and other advisory services, information and recommendations, but does not include an employee of a Councillor.

- **On-call Master Key ring** refers to a keyring made up of master keys for a specific building(s) for the on-call designated employee to complete maintenance/emergency calls.

- **Record Keeping** means all master documents of records of approvals of all issuances of access cards, keys and stock inventory are maintained and are consistent with procedures established by City of Brampton Security Services Department, the Brampton Records and Information Management System,and the Records Retention By-Law .

- **Temporary Users/ Daily or Temporary Use** refers to an employee or non-City staff temporarily signing out an access card from Security Services to use for the day, after which will return the card at the end of the day.

11. References and Resources

This Administrative Directive should be read and applied in conjunction with the following references and resources as updated from time to time. Please note that some of the following documents may not be publicly available due to privacy.

References to related corporate-wide procedures, forms, By-Laws and resources

can be found here:

- Keywatcher Touch Standard Operating Procedure
- Key & Access Control Program Overview
- Key & Access Request Form
- Key Replacement Form
- Key Authorization Form
- Records Retention By-law 272-2014

Revision History

Date	Description
2020/12/17	New. Approved by CLT on December 17th 2020.
2023/12/18	Next Scheduled Review

Attachments:

Schedule A: Security Zone Definitions

SECURITY ZONE CLASSIFICATION

Zone Classification	A - Public	B - Reception	C - Operations	D - Sensitive	E – Highly Sensitive
			Restricted Area Access Zones		
Definition	A Public Zone is where the public has unimpeded access and generally surrounds or forms part of a facility.	A Reception Zone is where the transition from a Public Zone to a restricted area zone is demarcated and controlled. Access by visitors may be limited to specific times of the day or for specific reasons.	An Operations Zone is an area used primarily for business operations. Access is restricted to personnel authorized to have access and to escorted visitors.	A Sensitive Zone is an area where access is restricted to personnel authorized to have access and to properly escorted visitors.	A Highly Sensitive Zone is an area where access is restricted to screened, authorized employees and to authorized 3rd party visitors.
Example	A Public Zone is the grounds surrounding a building or public corridors and elevator lobbies in multiple occupancy buildings.	A Reception Zone is typically located at the entry to the facility where initial contact between visitor and the department occurs; this can include such spaces as places where services are provided and information is exchanged. The perimeter may vary depending on the time of day.	An Operations Zone is typical open office area e.g. West Tower and City Hall office space	A sensitive Zone is an area where strategic information is processed or stored, that requires an elevated level of physical security controls e.g. Internal Audit, Human Resources, CAO office	A Highly Sensitive Zone is an area where high value, highly sensitive, or critical assets are kept and handled only by selected personnel, that requires a greater level of physical security controls e.g. IT server telecom rooms, Security Systems rooms
Physical Security Controls	Physical security controls may include, but not limited to: • Intercom • CCTV • Display of security/facility related signage and access points • Periodic Security Guard presence	Since the Reception Zone may transition based on the environment, the extent of controls will vary depending on the time of day or as indicated by a risk assessment or security review. Physical security controls may include items as described in the Public Zones, and also include the following: • Access Control • Periodic Receptionist/Security Guard presence at demarcation points • Periodic Security Guard patrols	Physical security controls may include items as described in the Reception Zone and may also include the following: • Periodic Security Guard patrols/posts • Security Guard/Authorized personnel working at the location<**authorized to challenge unfamiliar individuals**> • Working stations, offices, filing cabinets are secure when unattended • Physical security related standards and/or procedures • Perimeters must be physically sound and protected against unauthorized access.	Physical security controls may include items in the Operations Zone, and may also include the following: • Perimeter must be clearly defined/marked and strength of security requirements should be commensurate with the value of the information or information processing assets.	Physical security controls may include items as described in the Sensitive Zone, and may also include the following: • Access Control, which may include dual authentication • Static Security Guard patrols/posts • Intrusion detection • Alarm/event response • 3rd Party Vendor access control management.