Category: Administration Standard

Title:	**Access to Restricted Areas**
Approved by:	**Director, Corporate Security**
Effective Date:	**2024 October 23**
Last Updated:	**2024 September 16**
Responsible Service	**Corporate Security**

1. ASSOCIATED GOVERNANCE

1.1. This administration standard outlines requirements in support of the Loss Prevention Administration policy.

2. PURPOSE

2.1. This standard should be followed when employees interact with City workspaces that are not open to the public or all employees.

2.2. Following this standard will result in protection of personnel and property and minimize loss of, or damage to, City of Calgary assets.

3. DEFINITIONS

3.1. In this Administration *Standard:*

a) **"Employee"** means any person employed by The City and reporting to a City of Calgary business unit, department, the Office of the Chief Administrative Officer, the Office of the Chief Operating Officer, the Office of The Mayor, the City Auditor's office, the Calgary Housing Company and the Calgary Police Service, including those working under an employment contract with The City;

b) **"Supervisor"** means any employee with direct reports and supervisory responsibilities;

c) **"Threat risk assessment"** means a proactive assessment of a building or site used to develop a plan to identify and mitigate actual or potential risks;

d) **"Security review"** means a specific investigation in response to an identified security issue;

e) **"Social distress"** means emotional or psychological discomfort experienced by individuals or groups within a society due to various social factors such as isolation, drugs, discrimination, inequality, economic hardship, or political instability; and

f) **"Social disorder"** means events such as civil unrest, protests, demonstrations, political instability.

APPLICABILITY

4.1. This Administration Standard applies to all City of Calgary employees, except Calgary Police Service employees.

5. STANDARD

5.1. *Employees must:*

a) Use keys and access cards for personal access only;

b) Sign-in if attending a worksite after hours or at locations with supervised access;

c) Request access changes through their supervisor when their role changes;

d) Immediately return keys and access cards to their supervisor on termination of employment; and

e) Report unauthorized access, lost or stolen keys and access cards, and security incidents using the online forms from myCity or by contacting Integrated Security Centre at the phone number on their City identification.

5.2. *Supervisors must:*

a) Authorize (through Corporate Security) access to workspaces used by their teams;

b) Ensure employees are informed about the reasons for restricted access to areas;

c) Ensure the return of keys and access cards upon termination of an employee's employment;

d) Report new or changed risks to Corporate Security, Security Operations and Investigations; and

e) Respond to physical threat risk assessments and security reviews from Corporate Security, Security Investigations including securing budget for recommended resources and equipment.

5.3. *Corporate Security employees have their access approved:*

a) By business unit supervisors when specific access to restricted areas is required to fulfil assigned duties; and

b) By Manager, Security Risk Monitoring and Response when exceptional access to restricted areas is required to address sensitive, confidential or emergency situations.

5.4. *Security Operations employees will*:

a) Provide access to work areas through sign-in and/or keys and access cards;

b) Monitor public areas, including observation of available security cameras;

c) Monitor security systems alarms;

d) Provide initial emergency response to observed or reported incidents, including intruders, social distress, and social disorder;

e) Coordinate subsequent response to observed or reported incidents; and

f) Report security concerns and actions to Corporate Security Operations leaders.

5.5. Corporate Security Physical Security teams implement physical access controls, including sign-in, access card readers, and security door hardware.

5.6. Corporate Security, Security Advisors will conduct physical threat risk assessments and security reviews and report to supervisors on identified risks and recommend actions.

5.7. Manager, Security Risk Monitoring and Response will, as part of the response to sensitive, confidential or emergency situations, authorize immediate access to Corporate Security and/or specialized personnel to normally restricted areas as required to respond to the sensitive, confidential or emergency situations.

6. CONSEQUENCES OF NON COMPLIANCE

6.1. Employees who fail to adhere to this Administration policy may be subject to corrective action, including dismissal from employment, in accordance with the Labour Relations policy, the Exempt Staff policy, or the specified terms outlined in their employment

7. HISTORY

Action	Date	Approved by	Description
New Standard Rescind Policy	2024 09 16	Service Director	Replaces the former Access to Restricted Areas Policy. Standard approved be Service Director 2024-09-16. Effective 2024-10-21 when existing policy was rescinded by ELT2024-1146.
New	2006 07 31	ELT	New Policy
	1993 03 31	n/a	Chapter 7: Security (in the hard-copy-based editions of the Administration Manual)