



Document Name: Access Control Policy & Safety and Security Community Guidelines
Document Type: Policy & Guideline
Measure: WEPP
File Code: USEC
Last Update: October 2009
Pages: 7
Status: In Use

Purpose

To facilitate access to space and equipment by authorized users (staff, students, faculty, community guests and external parties) and in particular, to safeguard members of the Ryerson community and its physical assets, a policy on access control has been established. This policy and supporting guidelines sets out specific responsibilities, conditions and practices which are designed to address critical access needs in a manner which minimizes risks to personal safety and maximizes physical asset and private information protection.

Scope

This policy applies to all Ryerson individuals having responsibility for decision making regarding the use of space or equipment and authorized access to any Ryerson owned or leased space.

Policy Statement

The safety and security of the physical space and assets is a shared responsibility of all members of the University community. To meet this obligation, the University has established access control policy provisions to address the design, administration and management of access control systems and measures to ensure their integrity.

Policy

1. Access control, both allowing and restricting access to space and equipment, will be administered by the departments that are responsible for the space and / or the equipment contained therein and the safety of staff, faculty or students having authorization to use such space or equipment.
2. Access control for building perimeters will be under the direction of Security and Emergency Services.

3. The appropriate level of access control for the protection of users, property and private information will be determined by each department, in consultation with Security and Emergency Services and in accordance with safety and security guidelines established by the Center for Environmental Health, Safety and Security Management and the University's Personal Information Protection Guidelines.
4. Factors which must be considered in developing access control plans shall include:
 - isolated areas where people work alone or during low-traffic hours.
 - expensive devices, equipment or other property that could be targeted for theft;
 - sensitive information that should remain confidential;
 - equipment of which use must be restricted to authorized / trained users;
 - essential functions or processes which require uninterrupted conditions; and
 - research or other activity that should not be disturbed;
5. The level of access control is based on risk assessment and individual departmental needs, and will subsequently define the following levels of control measures:

Low level access control measures may include:

- installing locks and door plates that make unauthorized access more difficult;
- issuing keys to all room users, in accordance with conditions set out in the University Key Control Policy; or
- keeping rooms open and placing audible alarms or monitored alarms on equipment.

Medium level access control measures may include:

- issuing keys only to an access control designate within the department/office, who provides key access when needed; or
- installing security systems that are monitored by Security and Emergency Services on all access points.

High level access control measures may include:

- appointing staff such as lab monitors who are present while rooms are accessible;
- installing security systems that are monitored by Security and Emergency Services; or
- installing card readers on the perimeter as well as individual rooms.

All security systems and devices and related plans must be pre-approved by Security and Emergency Services

6. Every department shall appoint a person in the department who is responsible for coordinating access control and liaison with Security and Emergency Services on matters relating to the integrity of the related access control systems and measures.
7. Access during designated University closures, will be determined by the Executive Group, in consultation with Deans and Senior Directors. Departments will need to ensure that appropriate arrangements for access are in place for persons who are authorized to enter the University during designated closures. Such authorization must be approved by the appropriate Dean or Senior Director and include submission of an access control plan to Campus Safety and Security, by the Chair, Academic Director or Manager.
8. Access control plans must address the needs of faculty, staff and students with disabilities.

Roles and Responsibilities

Security and Emergency Services

Security and Emergency Services shall:

- direct and coordinate building perimeters access;
- be responsible for unlocking and securing all perimeters on campus;
- provide on-going assistance on matters relating to building and room access;
- establish and maintain current university-wide guidelines regarding access control and related security system measures;
- provide advice and recommendations to departments regarding the development and maintenance of access control systems and measures for their respective areas;
- provide advice, recommendations and project coordination for security systems design and installation; and
- respond to intrusion alarms that are monitored by Security and Emergency Services.

Individual Departments/Offices

Chairs, Academic Directors, Managers and representatives of Unions and Associations shall:

- establish an access control system, in consultation with Security and Emergency Services;
- provide access control for all the spaces that they are responsible for in accordance with the guidelines established by Security and Emergency Services; and
- implement the related provisions made under the Security System Alarm Protocol and Security Systems guidelines.

Departments who book space on behalf of internal or external client shall:

- make arrangements for access with the department(s) that are responsible for the space;
- establish an access control plan for the event or activity;
- communicate the access control plan at least 48 hours in advance of the event, to Security and Emergency Services, indicating perimeter access needs; and
- ensure that persons who have booked space are familiar with their obligations under the Security Systems Alarm Protocol Guidelines, where appropriate.

Jurisdiction

This policy is under the jurisdiction of the Office of VP Administration and Finance and is administered through the Centre for Environmental Health, Safety and Security Management.

Safety and Security Community Guideline 01-2004

Safety and Security Planning

Purpose

University policy 1-450 EHS Management System requires specific actions of all members of the Ryerson community in sharing responsibility for health, safety and security risk management. These actions include identifying hazards, becoming aware of risks inherent in activities and conditions which one may be exposed to and defining and participating in measures to ensure a healthy, safe and secure working, teaching and learning environment.

The purpose of the guideline is to outline criteria for establishing plans to address personal safety and security of members of the University community and protection of its assets.

Scope

These guidelines apply to all members of the Ryerson community, and are directed to those individuals having responsibility for decisions related to the use of space and equipment and authorized users within their respective areas.

Guideline

1. Directions for completing risk assessments are outlined in the Center for EHS and Security Management Risk Management guidelines and form. Risk assessments shall be conducted as conditions and activities change.

2. In consultation with Security and Emergency Services, a safety and security plan shall be developed and documented.
3. The plan will identify the following:
 - access control;
 - safety awareness and training;
 - environmental design;
 - safety and security communications;
 - security devices;
 - alarm protocols;
 - hazard/incident reporting;
 - emergency measures; and
 - contingency plans for community care and business continuity.

Roles and Responsibilities

All department heads and individuals in charge of an area shall ensure that a safety and security risk assessment and management plan has been established for activities and conditions within their respective areas. These plans shall be reviewed annually to ensure that they address current conditions.

The Center for Environmental Health, Safety and Security Management shall provide advice, assistance and services for the development, implementation and maintenance of risk assessment and management plans.

Safety and Security Community Guideline 02-2004

Security System Alarm Protocols

Purpose

False alarm activations divert security officer resources from emergencies and proactive programs. In so doing, false alarms place the safety of community members truly in need of security response in jeopardy.

Therefore, to reduce incidents of false alarms and thereby enhance community safety and security efforts, the following guidelines have been established to:

1. increase user awareness of the value of electronic security systems and their proper use as a crime prevention tool;
2. encourage the development of procedures and systems to reduce false alarm dispatches; and

3. develop and deploy standards and quality control measures to achieve responsible use of electronic security systems.

Guidelines

1. It is the responsibility of each department/office to ensure that the use of their security system does not cause disruption or draw emergency response resources from the university community. All false alarms caused by the department shall be noted by Campus Safety and Security and their frequency and related impact on resources shall be formally addressed by the individual department/Office.
2. Departments must ensure that they have in place effective access control and alarm activation/deactivation procedures, and that their employees and students are well versed in those procedures.
3. These procedures shall include:
 - details of alarm schedules;
 - listing of all those who are authorized to access the space;
 - procedures for notifying Campus Safety and Security of changes to alarm schedules and authorized users;
 - processes for advising occupants of the alarm protocols and procedures which outline their effective installation, implementation and maintenance; and
 - listing of department contacts in the event of access related emergencies.

Roles and Responsibilities

Security and Emergency Services

Security and Emergency Services shall:

- act in a timely matter on all reported security system problems and maintenance needs;
- ensure that all new security system installations meet the Center for Environmental Health, Safety and Security Management Guideline 02-2004 for Security Systems.
- implement procedures and system programming to prevent or cancel false alarms;
- advise and assist heads of departments/offices regarding their responsibilities relating to alarm system use and protocols;
- confirm, in writing to the department, the alarm schedule established by the department and the required procedures and measures to ensure its integrity; and
- ensure that when an alarm system is authorized for installation that the user department is notified of all related safety and security guidelines.

Responsibilities of Departments

Each department head or person in charge of an area shall:

- ensure that their users are educated on the prevention and causes of false alarms in order to successfully partner with Security and Emergency Services in security alarm protocols; and
- ensure that all users are thoroughly trained on how to operate their system, including knowledge of alarm status, time zones, access procedures, telephone numbers and procedures for notifying security when entering areas after hours, the process to cancel any accidental alarm, reporting any maintenance needs and advising Security of alarm schedule changes and how to ensure that all alarm points within their areas (windows, doors, gates etc.) are secure before leaving the area.