DALHOUSIE UNIVERSITY
Inspiring Minds

Department of Facilities Management

BUILDING SECURITY & ACCESS CONTROL

PERFORMANCE GUIDELINES – AUGUST 19, 2011

OBJECTIVE:

The objective of this guideline is to limit the probability that, as a result of the design or construction of a building, a person or property at Dalhousie University will be exposed to an unacceptable risk from unlawful or unwanted activity.

REFERENCES:

- Nova Scotia Building Code
- CPTED (International CPTED Association)

KEY STAKEHOLDERS:

- Facilities Management : Security Services
- Dalhousie University Community of Students, Faculty and Administrators

DEFINITIONS:

Access Control System (ACS) - an electronic system that allows, restricts and tracks the movement of people through entry/exit points in a site, usually achieved through programmable electronic keys, cards with readers.

Intrusion Alarm System (IAS) – a system designed to detect unauthorized entry or activity in a building or area. They consist of an array of sensors, a control panel and alerting system, and interconnections.

Remote Video Surveillance System (RVSS) - refers to a system or device that enables continuous or periodic video recording, observing or monitoring of activities in University controlled spaces. Monitoring of this system is at a distant location.

Security Services Command Center – refers to the center of Security Services operations, located in the McCain Building. This center is continuously staffed under the direction of a Shift Supervisor. This Command Center may be relocated to an alternate location due to an emergency event.

FUNCTIONAL STATEMENTS:

To achieve the objective of this guideline, the design and construction of a building shall enable Security Services to achieve the following functional requirements:

1. To identify and minimize the risks present in and around the building.
2. To identify and validate building occupants authorized for access to secure area(s) of the building.
3. To control the access of validated persons to the whole or parts of the building that are considered secure.
4. To resist the unwanted entry of invalid persons.
5. To provide Security Services situational awareness of developing risks in or around the building.
6. To minimize exposure of occupants to unacceptable risks.
7. To discourage illicit use of building and premises.
8. To contact the building occupants in case of emergency or potential hazard.
9. To compile usage data on building occupancy.

PERFORMANCE GUIDELINES

1. TO IDENTIFY AND MINIMIZE THE RISKS PRESENT IN AND AROUND THE BUILDING:

Provide a Preliminary Design Report which shall include identification of all risks and design recommendations, organized into the following table of contents:

1.1. Building Occupants, as indicated By Security Services in association with Bldg Administrators.
- 1.1.1. Intended uses and daily operation of building
- 1.1.2. Intended occupants and their expectations from Building Security System
- 1.1.3. Potential for unintended use or occupancy

1.2. Building Assets as indicated by Bldg Administrators, Security Services and EH&S Office
- 1.2.1. Identification of high risk assets
- 1.2.2. Hazardous Areas.

1.3. Potential Risk of Security Breach as indicated by Security Services.
- 1.3.1. Affect on Building Occupancy
- 1.3.2. Affect on Building Contents
- 1.3.3. Affect on Dalhousie University Operations
- 1.3.4. Affect on general public

1.4. Design Recommendations to Manage Risk:
- 1.4.1. Building Theory of Operation (Daily, Seasonal, Academic Year etc.)
- 1.4.2. Circulation
- 1.4.3. Compartmentalization
- 1.4.4. CPTED analysis including interior and exterior design
- 1.4.5. Access Control System Recommendations
- 1.4.6. Intrusion Alarm System Recommendations
- 1.4.7. Remote Video Surveillance System Recommendations

2. TO IDENTIFY THE BUILDING OCCUPANTS:

2.1. Identification of building occupants shall be accomplished through the Access Control System (ACS).

2.2. The ACS shall ensure that building occupants can be identified when entering the building.

2.3. The ACS shall provide user access through the University's single keycard (Dalcard) system.

2.4. The ACS shall be capable of independent subdivided control of any combination of the following:
- 2.4.1. Division by different groups of people. Some people may belong to more than one group.
- 2.4.2. Division by zones / building compartments. Compartmentalization ensures discreet areas have appropriate levels of security access.
- 2.4.3. Division by time and date.

2.5. The ACS shall have remote control capability from Security Services Command Center.

2.6. The ACS shall record the identity of the occupants and allow instant retrieval of this information by Security Services.

2.7. The ACS shall have a system administration function, allowing authorized administrators override controls. Administrative privileges shall be organized into hierarchical trees, with high level administrators collecting the privileges of subordinate administrators.
2.8. The ACS shall have a computerized log system which records all events.

3. TO CONTROL THE ACCESS OF VALIDATED PERSONS TO THE WHOLE AND/OR PARTS OF THE BUILDING:

3.1. The ACS shall provide automated door locking and unlocking based on section 2 above.
3.2. The ACS shall provide garage door entry control on a unified system.
3.3. The ACS shall permit locking and unlocking of all systems on an automated and flexible schedule. This automation system shall have remote control capability from the Security Services Command Center.

4. TO RESIST THE UNWANTED ENTRY OF NOT VALIDATED PERSONS:

4.1. Entrances and Exits from all Buildings / Compartments shall resist forced entry without dependency on house power or Access Control System.
4.2. The ACS shall report any attempts of unauthorized entry to Security Services Command Center including:
4.2.1. Failed access attempts.
4.2.2. Forced entry.
4.2.3. Propped doors.
4.3. ACS hardware components shall be of sufficient quality construction and design to resist vandalism and tampering.
4.4. Intrusion Alarm Systems (IAS) shall be provided in areas designated from the risk assessment, shall be integrated with ACS system to allow simultaneous monitoring, and shall seamlessly report to Security Services Command Center any system events including:
4.4.1. Forced entry.
4.4.2. Motion detection.
4.4.3. Security Sensors Alarms.
4.4.4. The system shall have a computerized log system which records all events.
4.5. IAS hardware components shall be of sufficient quality construction and design to resist vandalism and tampering.

5. TO PROVIDE SITUATIONAL AWARENESS OF DEVELOPING RISKS IN OR AROUND THE BUILDING:

5.1. A Remote Visual Surveillance System (RVSS) shall be provided in areas designated by the risk assessment and shall :
5.1.1. Connect seamlessly into the Access Control System (ACS) and the Intrusion Alarm System (IAS).
5.1.2. Be reviewable from Security Services Command Center.

5.1.3. Be capable of archival at the Security Services Command Center in full quality for future retrieval.

5.1.4. Be securely accessed by authorized Security Services personnel only. All access shall be recorded in a log.

5.2. All RVSS events, system information, and remote control functions must be remotely controlled and monitored at the Security Services Command Center in the McCain Building.

5.3. All RVSS Information shall be well integrated, organized, and displayed for fast and accurate Situational Awareness by the Security Services Shift Supervisor.

5.4. RVSS hardware components shall be of sufficient quality construction and design to resist vandalism and tampering.

5.5. All Systems including Access Control System (ACS), Intrusion Alarm System (IAS), and Remote Video Surveillance System (RVSS) shall be capable of rerouting to an alternate emergency Command Center.

6. TO MINIMIZE EXPOSURE OF OCCUPANTS TO UNACCEPTABLE RISKS:

6.1. All systems, hardware, and building design shall meet all Provincial Building Code and Municipal Bylaw requirements, including any special local requirements by all Authorities Having Jurisdiction.

6.2. Access Control System (ACS) shall permit remote control of Building / Compartment egress at Security Services Command Center during an emergency response including:

6.2.1. Unlimited Exiting – Unlock Building / Compartment to permit exiting during an event.

6.2.2. Lock Down – Locking to restrict entry into a Building / Compartment during an event.

6.2.3. Remote control system shall not allow violation of Building Code, Municipal Bylaws, or directives from Authorities Having Jurisdiction.

6.3. The ACS shall be connected to emergency power generation where available.

6.3.1. Where emergency power generation is not available, all components shall have a minimum (8) hour battery backup. All systems shall have integrated battery test system which notifies Security Services Command Center in event of low battery.

7. TO DISCOURAGE ILLICIT USE OF BUILDING AND PREMISES:

7.1. Building Design shall respond to the requirements of the CPTED analysis and Risk Assessment Recommendations to discourage illicit use of building and premises.

8. TO CONTACT THE BUILDING OCCUPANTS IN CASE OF EMERGENCY OR POTENTIAL HAZARD.

8.1.1. This section reserved for future use.

9. TO COMPILE USAGE DATA ON BUILDING OCCUPANCY:

9.1. All Systems (ACS) (IAS) (RVSS):

9.1.1. Location, time, and duration of Events.

9.2. Access Control System (ACS) shall record and archive the following data:

9.2.1. Identity and time of an individual making a request to access and reason for access denial to a building / compartment.