UNIVERSITY OF TORONTO | Facilities & Services

# Security and access control systems design standard

Revision 03

Last updated: August 14, 2025

UNIVERSITY OF TORONTO | Facilities & Services

**Table of contents**

## 1. General

1. The Client (University of Toronto St. George Campus) utilizes an integrated security system to manage physical security to the community. All projects related to physical security shall adhere to this standard.
2. This standard shall be read in conjunction with the deliverable standard. Any deviations shall be documented in the building design standard variance request form and be reviewed with the Client.
3. The security system shall integrate the following components:
    - Physical access control and credential
    - Intrusion alarm detection systems
    - Video Surveillance (CCTV)
    - Emergency help stations
    - Panic alarm systems
4. The security system shall be monitored 24/7 for alarms.
5. The security system shall use the Honeywell Enterprise Building Integrator (EBI) software platform in conjunction with PCSC fault tolerant devices and controls as the core operating system. Only controllers and end devices that are compatible with the security system shall be used.
6. The security system shall operate entirely on a closed private Facilities & Services (F&S) network. All new physical security system projects shall be connected to the F&S network.
7. A kick-off meeting shall be scheduled with the Client's security representative and Architect during the design phase.
8. The Architect shall engage the Client's Lockshop during design reviews and commissioning phase. Refer to the Client's building commissioning standard.
9. The U of T Lockshop shall commission all projects for security and access control systems.
10. All installed hardware shall include a minimum two-year comprehensive warranty, effective from the date of commissioning report approval.
11. The use and procurement of any equipment covered under the U.S. National Defense Authorization Act (NDAA), 889(1)(B) is prohibited. Architect shall follow the most current list and make updates throughout the project's design process.

## 28 10 00 Monitored physical access control

1. Monitored physical access control is a type of physical access control system that authorizes or restricts entry to spaces such as buildings, rooms, or secured areas. The system shall be centrally monitored for alarms.
2. The following access points shall be integrated into the security system:
   - Entrance and exit doors, as well as any interior doors identified by the Client
   - Data rooms
   - Elevator machine room and pit door(s)
   - Elevator cabs (for floor access control)
   - Classrooms managed by the Client's Learning Space Management
   - Entrances and exits to electrical substations and generator rooms
3. All security system connections shall be hardwired.
4. Doors shall be equipped with electric lock. Electric strikes are not permitted.
5. Locksets shall be electric with built-in Request to Exit (REX) functionality.
6. Door contact or door position switch shall be minimum 20 mm (¾ inch).
7. The use of magnetic locks (mag locks) within the security system must be reviewed by the Client.
   - Mag lock can only be used on interior doors
   - Mag lock reset switch shall be installed adjacent to the fire alarm annunciator panel
8. All credentials[1] shall be purchased through the Client (Campus Safety) by project.
9. For lock hardware requirements, refer to door hardware design standard.
10. Standard of acceptance:
    - Controller: PCSC fault tolerant controller with single door module or dual door module.
    - Card reader: HID branded reader. The current standard model is HID Signo line. MOB key 0180.
    - Credential type: HID keyfob II, 32-bit class.

## 28 20 00 Video surveillance[2]

1. All camera placement designs shall be reviewed by the Client.
2. Project shall include video surveillance design for all perimeter doors to the building. Camera shall be placed on the interior side of each perimeter door.
3. Signage shall be posted in proximity to the camera and/or at building entrances where video surveillance is active. Signage template will be provided by the Client to Project Team for fabrication and installation. Signage shall be used only in areas that are recorded within the F&S security system.
4. Departments or faculties may request dedicated viewing station(s) to view cameras located within their respective areas. The views will be live ONLY, no recordings.

[1] Credential refers to a device that activates an electronic reader, which in turn enables the system to activate a mechanical device or disengage a lock, permitting access to a secured area. Common credentials include access cards or fobs
[2] Video surveillance refers to the digital recording of a defined space or area.

5. Video surveillance data shall be retained for 30 days on F&S servers. Access to recorded footage is restricted to authorized Client (Campus Safety) personnel.
6. Standard of acceptance:
    - Cameras: Power over Ethernet (POE) and Axis branded cameras. Current standard models are Axis P and Q series.

### 28 30 00 Security detection, alarm, and monitoring

1. Intrusion alarm systems shall consist of controllers, sensors and keypad(s) that actively monitor designated space(s) and assets(s).
2. All controllers and keypads shall be hardwired.
3. Sensors and contacts can be wireless.
4. Standard of acceptance:
    - Honeywell Vista intrusion alarm systems

### 28 40 00 Life safety

1. Panic button systems shall provide a direct alert to the Client (Campus Safety) in emergency situations. It is required to implement these systems in areas with potential for escalating interactions, such as reception desks, information counters, and gym access points.
2. Each panic button system shall include both a panic button and a camera, with the button positioned within the camera's field of view.
3. Standard of acceptance:
    - Camera: Axis P3265-LVE
    - Button: Honeywell 270R Hold-Up Device

### 28 55 00 Emergency help station

1. Emergency help stations shall provide direct two-way communications with Campus Safety when assistance is required.
2. Location(s) for emergency help stations design shall be in parking garages and exterior areas where paths of egress are restricted, such as surface parking lot with only one entry/exit path.
3. Installations shall be clearly marked with "EMERGENCY" lettering on pole or box and include a blue light.
4. Standard of acceptance:
    - 2N IP Force

### 28 05 13.01 Security system cabling

1. All hardware shall be connected via POE from device to F&S switch. This shall be read in conjunction with the Client's Networking Hardware and Cabling standard, and Building Automation Systems Design

Standard section 3.19.2 building automation – data cable, 3.19.3 wiring installable qualification document, 3.19.4 Fluck reports requirements.

2. For wiring requirements for the physical layer networking – building security end devices, follow the requirements in the Figure 1 below.

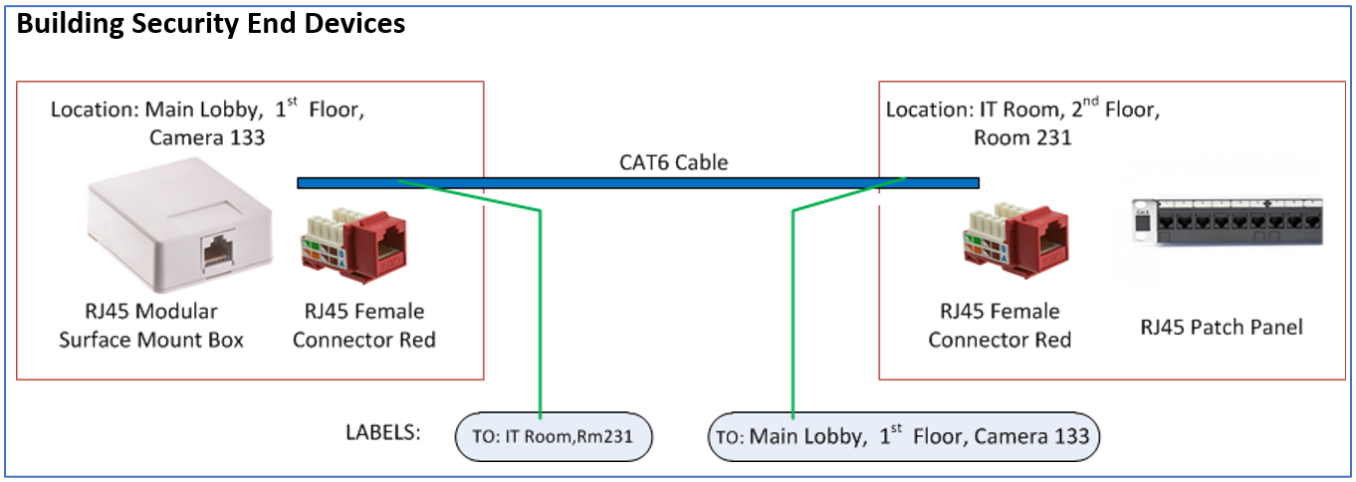


*Figure 1 Building security end devices*