



impro technologies®  
ACCESS CONTROL

# Keeping education **SECURE**

*Best practices to help keep students, faculties and staff safe*



[www.impro.net](http://www.impro.net)

ACCESS CONTROL

# Six step strategy

1. Assess and plan
2. Central entry point
3. Know who's inside
4. Develop surveillance
5. Limit visitor access
6. Use of access control IDs



## Strategies to improve security and safety

While educational institutions remain one of the safest places for students to be, increase global trends and crime are leading parents, students and the community to believe otherwise.

Perception can be more powerful than reality, to the detriment of student enrollment, academic performance and staff morale.

The best way to begin addressing these fears is to be prepared with a plan, and create an open dialogue with the various stakeholders.

Ensuring the safety and security of an institution isn't the role of a single person, nor can it be achieved with one single action or method of control.

Creating a safer environment requires a comprehensive prevention and response strategy that actively involves students, parents, staff, faculty and community.

# Strategy 1: Assess and plan

Developing an emergency plan that considers a variety of potential dangers to your learning environment is the first step in protecting your students.



# Where to begin

The first step in creating a safer, secure facility is conducting an assessment to determine current threats and vulnerabilities. While pre-planned, armed attacks may be top-of-mind, you should also consider threats such as man-made disasters, infectious diseases and illness, natural disasters and abductions.

Once you identify the factors that could have the greatest impact on your facility, you should develop an emergency operational plan to address them. Then you'll be in a better position to prioritise your efforts and resources.

## Step 1: assemble your team

Your team should include local law enforcement and emergency response services, plus representatives of all stakeholders in the school, such as the school board, administration, staff, students, parents and community members.

Many institutions also hire a consultant to guide them through this assessment process.

## Step 2: conduct the assessment

Begin with a walkthrough while school is in session, to better evaluate your day-to-day security operations in action.

It's best to start in an adjacent area to the educational facility and follow the path students and visitors take, up to the entrance and through to the classroom or lecture hall.

Observe with a critical eye - look for things such as where people could hide; whether vehicles are visible from the entrance or front office; if there are structural or natural elements a person could use to climb up onto the roof; and if your existing security, lighting and/or CCTV equipment is fully operational.

## Step 3: uncover threats and vulnerabilities

Assessments should document two primary things - threats and vulnerabilities. Threats are external events that put people and/or property at risk, while vulnerabilities are gaps in your facilities, policies and procedures which threats could potentially pass.

Your assessment team needs to prioritise which threats and vulnerabilities represent the greatest risk so you can design a plan for mitigation.

## Step 4: build your emergency plan

An emergency plan outlines how you intend to mitigate the threats and vulnerabilities you identified in the previous steps. It should:

- List your community partners, such as law enforcement, first responders, mental health providers, hospitals and more.
- Specify the roles and responsibilities of those partners, as well as your own faculty and staff.
- Identify any training needs, both internal and external.





A black and white photograph of three men in a library setting. They are gathered around a table, looking at a laptop screen. The man on the right is pointing at the screen and smiling. The man in the middle is wearing a baseball cap and glasses, also smiling. The man on the left is partially visible, wearing a cap and glasses. In the background, there are bookshelves filled with books. A red rounded rectangle is overlaid on the right side of the image, containing the text for Strategy 2.

## Strategy 2: Central entry point

Limiting and monitoring entrances reduces the opportunity for criminal activity, while limiting the cost to secure your educational facility.

The easiest and **most important action** an educational facility can take to become more secure, is to drive all visitor and unbadged traffic, including students and staff, to a centrally located, easily monitored entry point.



The entry point should be manned by security or other front-office personnel and equipped with one or more CCTV cameras. Visitors should also be required to exit the same way they entered and to check out before they leave the building.

**Staff the entry point with security or front-office personnel**

Visitors, meaning anyone without a badge, should be identified, verified and badged before entering the building.

Best practices recommend requiring a government-issued ID to be presented, before a temporary visitor badge is issued.

**Where possible, create a physical barrier**

Many schools use a security vestibule, hut or double entry system which allows staff members to screen guests before granting them access to the building.

Some schools are going further, building restrooms and small conference rooms outside the "firewall" to accommodate visitor needs without impacting security protocols.

**Lock down all other potential entry and exit points**

Use locks or other hardware to prevent access to the building from the roof, windows or vents. Make sure no structures or building features could allow climbing access to adjoining windows or roofs. Further, fit all exterior entries with hardware that facilitates a full perimeter lockdown in an emergency.

*Remember to keep a watchful eye.  
All staff should be trained to not allow an unknown person follow them into the institution, without being formally checked in.*



# Strategy 3: Know who's inside

An effective visitor management system and process improves the safety and security of students and staff.

Identifying and badging visitors to your educational facility can be labour-intensive and time consuming. As a result, many are choosing automated visitor management systems which can complete verification and badge printing in just a minute. Schools can then manage who enters the building, when and for what purpose, while reducing the staff time and energy to do so. Parents can also be assured that administrators know who has access to their child's school.

Manual visitor management is vulnerable to risks. Paper visitor books and logs, while simple and seemingly efficient, present a number of security risks:

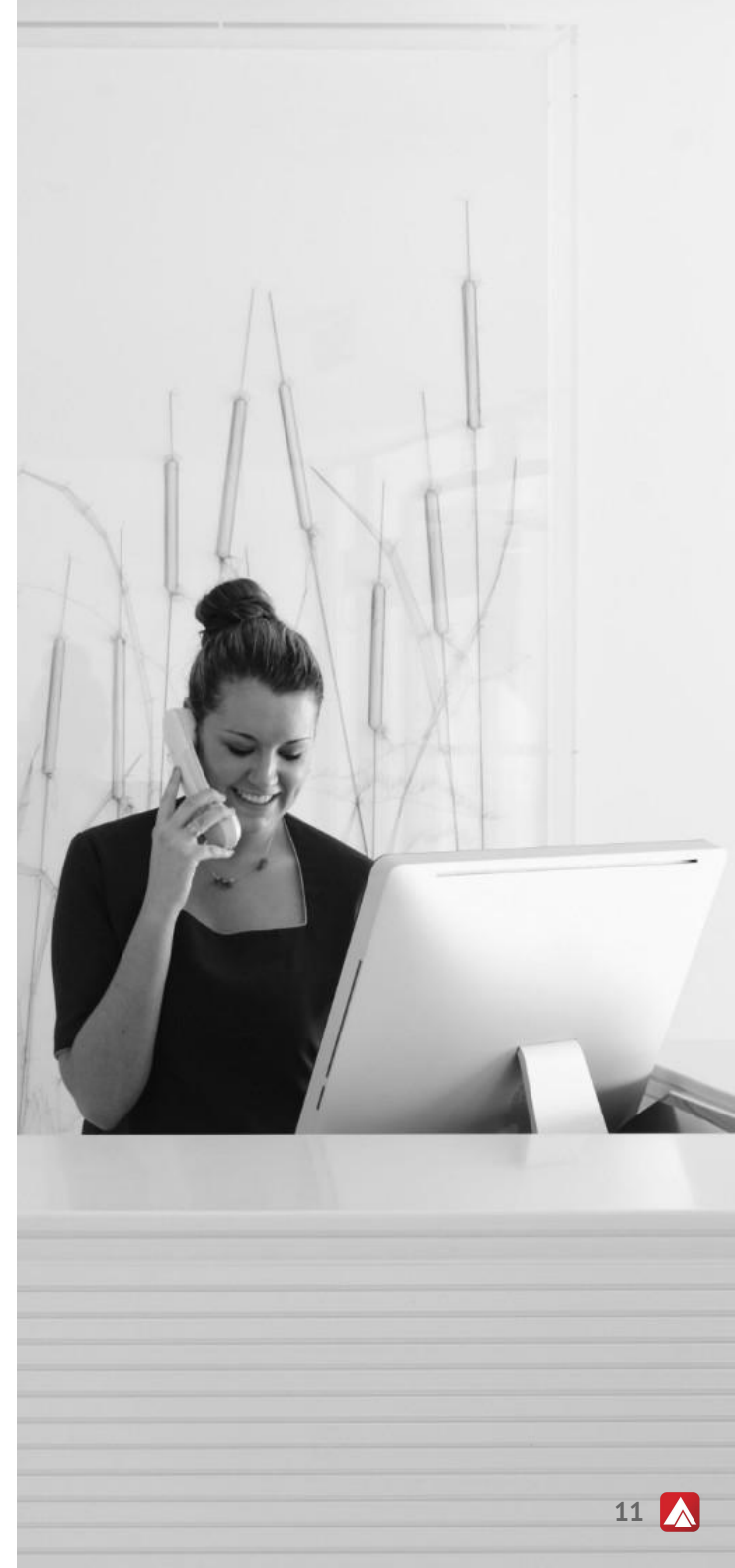
- Visitor information can be easily falsified. Visitors can easily see who has preceded them into the building.
- There's no way of knowing if they are allowed access to the premises, or were previously blocked.
- In an emergency, it's difficult to know who's in the building or where they are.

#### **Automated visitor management systems help ensure security**

With an electronic system, visitors present a government-issued ID, such as a drivers license or identity document, which can be scanned and screened against internal watch lists. The system then provides a high-quality, customisable badge which can even include the visitor's photo - in just a few minutes.

In addition to speeding up the visitor management process, an electronic system can also:

- Alert security or reception about visitors before they arrive, as a web-based interface allows for staff to pre-register guests so front-office personnel know who will be arriving that day and when.
- Act quickly in an emergency. You're able to determine precisely who's in the building and where, with the click of a mouse.
- Streamline future visits. The system can use information captured in the database to recognise previously verified visitors.
- Facilitate a review of patterns. Administrators can quickly access visitor reports to identify patterns or opportunities to improve visitor management procedures.
- Enhance your institutions' professionalism. Internal databases can be used to identify VIPs or board members, helping front desk staff better assist them when they arrive.







## Strategy 4: Develop surveillance

Together, formal and informal surveillance can provide a powerful deterrent and thwart potential threats before a crisis occurs.

# Core principles

## **Formal surveillance**

This refers to CCTV, access control and other electronic equipment used to monitor entrances, parking areas, hallways, playgrounds and more for suspicious activity.

## **Informal surveillance**

Often called "eyes on the street" this refers to the watchfulness of faculty, staff and students who are highly attuned to the flow of people and activities in their areas and buildings.

## Developing your formal surveillance

### Use appropriate equipment

Security equipment experts recommend point-tilt-zoom (PTZ) cameras because they can cover more space, meaning you may be able to use fewer cameras. It's also recommended that IP cameras are used, for increased resolution and lifespan. The cameras should be positioned to show visitors' faces and offer good sight lines down hallways and into stairwells.

### Monitor the entry lobby

Even with a staff member present, video surveillance helps monitor and prevent the practice of "piggybacking" through access controlled areas. This is when an unauthorised and unscreened person gains access to the building behind a student or staff member.

### Don't forget the hard-to-see areas

Parking areas, drop-off zones and other exterior areas may be difficult or impossible for staff to monitor from the front office or main entry. But awareness and monitoring of these areas may provide an early warning that something is amiss.

## Encouraging informal surveillance

CCTV and access control systems are only part of the solution. Informal surveillance, which relies on the attentiveness of students and staff, often provides the first indication that something, or someone, is out of place.

It begins with a simple, intuitive awareness of who and what belongs in the building, and who and what does not.

To enhance the effectiveness of informal surveillance, staff should receive regular, ongoing training regarding school policies, procedures and action plans.





In an international study of architectural, engineering and construction professionals, 69% said they have specified or installed CCTV and electronic security systems for educational facilities in the past 18 to 24 months.

# Strategy 5: Limit visitor access

One teacher or student propping open a door, can negate the millions spent on a security system.



Learning institutions, like any facility, can be divided into securable zones. Students, staff and visitors can be given access control smart cards which allow entry only to the appropriate areas. Going a step further and color-coding the visitor cards, will alert people whether the visitor is supposed to be in a secured zone, or if they need to notify security.

Granting or denying access, based on information coded into the access card, also prevents opportunistic crime. Perpetrators, when faced with a series of locked doors, often abandon their plans and simply move on in search of an easier target.

#### **Create clear zones of space**

Educational facilities are often used for a wide variety of community functions.

To limit public access and improve security, many facilities divide classroom zones from community areas, so visitors can enter the community space and not the classrooms. Within the classroom zone, some

visitors might receive access to hallways in order to undertake repairs, for example, but will be denied access into the individual classrooms.

Within the classroom zone, some visitors might receive access to hallways in order to undertake repairs, for example, but will be denied access into the individual classrooms.

#### **Training**

Training your staff is just as important as upgrading your access control system or implementing zoning principles. While things like electronic access control, smart access cards and associated door hardware are critical to keeping a campus secure, staff training and adherence to policies is equally critical.

Situation awareness, or simply being aware of what's going on around you, also goes a long way. The sooner you're aware of potential danger, the better.

*In a USA survey, 40% of respondents said students and staff "are not trained on access control policies or don't follow them"*

## Strategy 6: Use of access control IDs

In addition to identifying students and staff, access cards/IDs can perform other functions that help streamline student and personnel management.







## One card that does it all

Access control ID badges can perform more than simply allow access to an area.

Rolling visual identification, student enrollment, dorm rights and food service capabilities into one single badge, makes it easier for students and administrators to track and manage important daily functions.

These could include:

- Time and attendance.
- Employee management software, such as PeopleSoft.
- Student accommodation or transportation.
- Canteen and catering services.
- Transactions at libraries or bookstores.

In a facility with hundreds or thousands of students, along with staff, eliminating manual tasks in favour of digital solutions, saves valuable time and resources.

Even student enrollment can be streamlined and long queues removed, while increasing the convenience of enrolling and badging in minutes.

**Transportation**

Staff can easily track student whereabouts as they enter and exit school transportation with a handheld mobile reader.

**Time and attendance**

Identifying and recording student attendance used to be a paper-and-pen task. With access badges, information can be stored in a barcode, magnetic stripe or smart card, and when they swipe as they arrive, the system automatically records their arrival time. The same procedure would occur when they leave.

The same principle works for staff, whereby detailed reports can be drawn on their access, which is integrated into the payroll system, for one seamless management tool. Automatic rules can also be established, for example for contract teachers, whereby their access is automatically revoked based on their contract duration.

**Canteen and tuck shop**

Students are no longer required to carry cash or worry about theft, as the card can be preloaded with money. Students who receive free or reduced price food swipe their card like everyone else. No one but the system knows how much money each individual has in their account, preserving student privacy.

**Other transactions**

Learners can use their badges to "pay" for things such as library material, computer usage or school merchandise. The same card can also provide access to student accommodation.



# Partner with the leader in access control solutions

Impro Technologies has been pioneering access control solutions for over 30 years. We're a global provider of secure solutions that encompass hardware, software, various cards and access badges, card readers and biometric solutions.

We're also proud to partner with educational institutions around the world. Making your facility safer requires a multidisciplinary approach that combines technology, hardware and an ongoing commitment to training.

While no one piece of the puzzle can meet all your security needs, any small gap in your solution can put people and assets at risk.

We help evaluate your current strategy and provide guidance on a solution to promote your strengths and mitigate any weaknesses.



**Impro Technologies** has  
over 30 years' experience in  
the access control industry

HQ tel: H+27 (31) 717 0700  
Email: [info@impro.net](mailto:info@impro.net)  
Web: [www.impro.net](http://www.impro.net)