Security101

Modernizing employee and visitor management

In public institutions

Governmental entities, including *federal*, *state*, *municipal*, and *local agencies*, face the challenges of optimizing visitor flow of traffic and improving employee access.

Security101

Contents

Security101

Introduction

Governmental entities, including federal, state, municipal, and local agencies, face the challenges of optimizing visitor flow of traffic and improving employee access. Having a speedy and smooth access control system is vital, especially when the public sector tends to have a reputation for slow customer service, long waits, and lengthy procedures.

Nevertheless, a structured access plan to improve high-traffic in buildings is not sufficient.Today, it is necessary to have, in addition, clear and defined safety protocols in place that reduce the spread of viruses and satisfactorily protect visitors and employees from contamination agents.

This is easier said than done. An effective approach requires modern security innovations, expertly integrated, as well as touchless means of access. The goals are to harden the security of public institutions, protect people and assets from criminal activity against these organizations, improve user experience, and enhance identification and authentication methods.

Governing bodies have the responsibility of making people feel safe; however, they should also avoid security theater. True safeguarding is achieved by properly deploying first-class solutions that streamline admission processes and guarantee the protection of those who visit and work in the building, all while assisting citizens and workers safely perform their duties.

Access control functionality

To streamline employee and visitor management, municipal structures must adopt robust access control solutions that permit only authorized persons to enter and exit, deny entry to unauthorized individuals, prevent access of weapons, explosives, and other dangerous tools, and notify security teams of intrusion attempts.

Careful integration of access control with video surveillance and intrusion detection platforms is a valuable strategy that can enhance functionalities. Unification of these elements results in amplified visibility, holistic situational awareness, and more appropriate decision-making.

Access control should be deployed at the perimeter of the institution, and continue at building entrances and other sensitive areas. It must be tailored to the demands and unique requirements of each government agency, which often necessitates the four elements of access control:

1. Physical barriers
2. Authentication devices
3. Management system
4. Communications infrastructure.

In addition, a modern access control system allows government officials to remotely retrieve data related to suspicious activity and user permissions. When an issue is detected by the system, it is fundamental that a professional security team assesses and responds timely to threats.

FACTORS TO CONSIDER

Some factors to bear in mind when acquiring a new access control system are:

- What are the specific threats facing my organization?
- Can the new solution be integrated with my existing security systems (e.g., video surveillance)?
- How many access points will require coverage by this new technology?
- What are the highest value assets that need to be safeguarded (e.g., material property, intellectual property, classified intelligence)?
- What areas in the building are the most vulnerable?
- Does access control need to be intensified in certain zones?
- Does this solution require a centralized network system?
- Can the system be managed remotely?
- Is there a written policy for evacuation and will the access control system be used for mustering?
- Will the system integrator provide us with adequate training to operate the system?
- Is the solution reliable?
- Is maintenance cost-effective?

AVOIDING SECURITY THEATER

Security theater is a concept that refers to strategies used to make people feel safer without doing anything to actually improve their security. Courthouses, public works, public libraries, city halls, police stations, and fire departments, among others, cannot deploy countermeasures to security threats without first understanding and addressing their building's own specific risk posture.

Understanding what security theater means is key to avoid it. This is especially important when the entity is ready to invest in security equipment. In response to current threats against municipal structures, determining what solutions are truly securing the building and protecting the lives of visitors and employees is crucial.

The risk of an attack should be assessed from the moment citizens enter the building to how they interact with other individuals and employees on-site. A modern and effective access control solution should be adopted to genuinely provide value to the institution.

VULNERABILITY ASSESSMENT

The needs of a police department greatly differ from those of a city hall. Factors to take into account when determining current security risks, specific vulnerabilities, and new technologies to use are:

- Number of visitors served.
- Public accessibility to online procedures.
- Type of interactions that take place.
- Average time a visitor spends in the building.

Not all solutions are a good fit for an organization; therefore, public offices should consult aprofessional security team to take the decision that best serves their unique demands.

Employee and visitor management solutions

The countermeasures against criminal activity and intrusion should be both technological and procedural; further, they should focus on providing visitors and employees with a comfortable and fast admittance experience.

Hence, it is critical to conduct an extensive evaluation of how effective a technology/procedure is at eliminating actual security risks. This is essential to avert security theater and avoid spending money in physical security solutions that do not offer a significant impact on the building's risk posture.Monitor specific users.

MODERN PHYSICAL ACCESS CONTROL

Many governmental facilities continue to meet their access control needs with security guards and identification badges or a turnstile system. However, as every public organization should strive for secure premises, modernizing the access control system is vital to help administrators reinforce zone restrictions, improve on-site security, and simplify the admission of employees and visitors.

Deploying a solution that prevents full accessibility and limits permissions based on predefined criteria can improve zonal security. In addition, a sophisticated access control system can mitigate threats and increase productivity, as security teams can work more efficiently, requiring less staff.

Most importantly, the right solution helps officials be aware of access rights and privileges data, streamlining employee turnover. Some access control systems can be integrated with directories, which allows for automated provisioning and de-provisioning of credentials. This valuable feature, reduces maintenance, manual tasks, and human errors.

When credentials — key cards, fobs, keypads, and smartphones — are presented at a card reader, doors unlock, and authorized individuals get permission to be on the premise. Likewise, a management portal, controlled by leaders, the head of security, or IT managers, permits customization of the parameters of persons allowed to enter, and under which circumstances they can do so.

Access control is arguably the heart of all operations within your public organization. When this technology is cloud-based, the benefits go beyond physical building security and extend to a better user experience, simplification of access management processes, and remote administration, from any internet-ready device.

Benefits of a cloud-based option:

- Administrators can now control who has access to the public building and when, without the need to be on the same location.
- Digital encrypted credentials protect employee data.
- There are backup and disaster recovery capabilities.
- Enhanced security.
- Simplified management.
- Improved security.
- Scalability.
- Easier integrations with any third-party system.
- Automated workflows and updates.
- Centralized data management.

BIOMETRICS

Authentication through biometrics involves using some part of the physical makeup of individuals to verify they are who they say they are. This technology compares physical or behavioral traits to stored, confirmed, and validated data in a database to confirm a match and manage access to public buildings.

One of the types of biometrics is facial recognition that uses one or more photographic images to recognize a person by measuring points on a face, under controlled conditions. These systems are non-intrusive, do not demand contact with the user, and have a high rate of user acceptance.

As public organizations are particularly concerned with promoting and respecting equality and diversity at the workplace, facial recognition is a suitable alternative since it is not affected by race or gender-based differences in appearance. Facial recognition is an innovation that works well indoors, where most environmental factors, including lighting, can be controlled.

The cameras must be placed in strategic locations to ensure image quality. Other biometric authentication methods that can be used to facilitate access of employees and visitors are iris recognition, fingerprint scanning, hand geometry recognition, ear authentication, and signature recognition.

WIRELESS LOCKS

Wireless locks can help protect life and property at government agencies. Modernizing a site for improved security requires a system that can be managed remotely and that offers high levels of control and flexibility. This can be achieved by adopting a smart access control system as well as utilizing wireless locks.

As the world starts to normalize and public offices are again open to the public, safety, health, and hygiene are top priorities for decision-makers. The need to open doors, in the safest way possible, should be addressed with modern, automatic methods that allow visitants and workforce to unlock doors directly from an application on a smartphone, waving a hand in front of a reader, using a fob or a card, or touching the reader with a clothed area of the body, like the arm.

Ideally, individuals are not required to touch door handles or use keys to get access. A wireless lock approach provides a germ-free, touchless, ADA-compliant option that can guarantee the safety of everybody in the premises. Wireless, keyless platforms are a more sanitary option as they offer programmable and remote features, impossible to achieve by mechanical solutions.

These are some capabilities found in a wireless lock system:

Remote access

Administrators can lock/unlock doors from anywhere, using a mobile device, a smart credential, or a biometric feature.

Security

Lock-downs can be deployed remotely.

Convenience

Lost and stolen keys are no longer a problem. With the click of a button, public functionaries can issue or revoke secure credentials to any user.

Better UX

Employees can use their smartphones or a smart card to access the facility.

Streamlined visitor access

Citizens can enter the building at a scheduled time, by accessing a link sent via email or text.

Customization

If a staggered schedule for employees is arranged for, permissions and schedules can be determined. This system is easy to navigate, which facilitates making the appropriate changes, delegate permissions, and keep the access to the building safe and healthy.

Notifications

Alerts of any access event are sent to authorized individuals in real-time.

ANTIMICROBIAL DOORKNOBS

Other specialized technologies are helpful to protect people in governmental structures. An efficient solution is antimicrobial doorknobs made with bacteria-growth protecting technology, so even in the case that staff and visitants touch doors or other surfaces, they can be provided with a much safer environment.

In a public institution, as citizens come and go every day, this solution might be especially relevant, since it is not always possible to designate someone to the task of cleaning doorknobs all day long. Using this innovation can assist administrators in providing built-in antimicrobial protection.

The efficacious coating lasts the lifetime of the door lever and protects against bacteria growth. Interior design does not need to be compromised in order to have a safer environment. This is a solution that can be deployed in different public entities, including courthouses, which are known to have highly aesthetic spaces, with custom mill work, furnishings, and upholstered seats.

Security101

Conclusion

Government bodies often struggle with employee and visitor access management. Therefore, they require proper protocols and technologies to safely manage the flow of people, while keeping premises protected. Acquiring a modern access control solution is paramount for public institutions as it can streamline admission processes while enhancing the security of the institution.

Public agencies must ensure they are safe places, easy to navigate. Preventing unauthorized individuals from entering the organization guarantees that security is enhanced. Modern access control systems can allow remote management, verify employees, limit access to critical zones, keep confidential information safe, while maintaining public access to other areas. Moreover, wireless locks can support the efficacy of an advanced access control platform.

Without the right physical security solutions, governmental facilities might not be fully equipped to serve citizens and grant entry to employees in a fast and safe way. A qualified deployment and integration of a cloud-based access control technology can increase compliance, awareness, and safety. Administrators should also rely on the expertise of security professionals to avoid security theater outcomes and protect, undoubtedly, their workforce, and the people that utilizes their services.

FIND A LOCAL OFFICE

Contact your local office today for an on-site, no-cost security assessment.
For more information call 800.261.2041 or visit security101.com