



impro technologies®
ACCESS CONTROL

Three reasons to upgrade your **Access control technology**

www.impro.net

ACCESS CONTROL

*New technologies enable
a wide range of high-value
applications, from mobile
and virtual credentials,
to cloud technologies,
cashless vending and
secure print management.*

Introduction

The security landscape continues to evolve in new and complex ways. This evolution brings change on many levels, which offers an opportunity for improvement rather than an interruption or a distraction.

This concept has never been more important as you face today's combination of new technologies, escalating security threats and the need to derive greater value from the access control infrastructure, while solving increasingly complex system integration challenges.

Upgrading from older, legacy technologies to a new access control system is a significant

initiative. However, recent advancements have made this transition easier.

Today, you can move to more dynamic access control solutions which provide greater value, whilst also taking advantage of enhanced functionality and a higher level of security.

Access control has moved to integrated solutions with multi-layered security that includes multiple facilities.

These new technologies enable a more dynamic solution, allowing you to embrace new levels of convenience and utility.

In addition, you need to be considering the needs of tomorrow, rather than simply the requirements of today.

While the initial motivation to adopt a new access control system may be to improve security or to consolidate multiple locations under a single standard, it is the perfect time to build a foundation for addressing unanticipated future change and evolving security threats.



1. Data privacy

Data privacy

As a result of new legislation or regulatory requirements, your organisation may be required to increase its security, either to protect yourselves or the parent organisation.

Implementing a new, more dynamic access control solution provides many benefits over maintaining older, legacy systems.

Today, businesses face an environment of evolving threats, and the challenges of maintaining the security and privacy of identity data is ever greater.

In addition, the growing demand for a higher level of security and convenience of using mobile devices for access control is driving change and spurring innovation.

However, the unfortunate reality is that sometimes it takes an unexpected event or security breach to prompt an organisation to upgrade the access control system.

By making the right steps in moving toward a more reliable, upgraded access control solution, you can meet the need for security and privacy with confidence, and leverage your investment well into the future.

2. User convenience

User convenience

The freedom to move access control to smartphones, tablets, wristbands, watches and other wearables offers increased choice and convenience for end users, along with new and more convenient ways to open doors and gates.

Today, smart devices are always on hand. Users don't have to maintain and carry multiple cards and credentials.

For example, the longer reach of the Bluetooth Smart communications standard makes it possible to drive up to a gate without having to roll down the car window and reach out to activate a reader.

Some smart device sensors also enable gesture detection.

This offers an additional benefit for access control with the ability to open doors from a distance by performing intuitive gestures.

When one considers that it is predicted there will be nearly 155 million smart wearable devices in use by 2019, these "always-on" devices are ideal for access control applications because of the ready-to-use convenience as well as the reduced chance of loss.



3. Flexibility



Flexibility

Organisations need a system that is flexible enough to support multiple applications for managing not only physical access but also logical access (e.g. computer/software login, time and attendance, etc.) as well.

Organisations that want to add new applications, such as time and attendance, secure print management, biometrics, cashless vending and more, will need to issue an associated card to users.

This requirement can be used as an opportunity to migrate to other technologies that combine access control with these or other functions, enabling employees to carry a single device for many purposes.

Administration of these functions should be centralized into one efficient and cost-effective solution to enable you to create a fully interoperable, multi-layered security solution across company networks, systems and facilities.

In the future, you can migrate to the convenience, editability, and security of carrying digital keys and credentials on smartphones and other mobile devices.

Data privacy, user convenience and flexibility go hand in hand

Organisations are having to keep up with a variety of technology changes that impact the physical access control infrastructure.

These changes include accommodating two-year PC refresh cycles, 18-month average mobile device lifespans and policy changes surrounding the move to “Bring Your Own Device” (BYOD).

Additionally, there is increased network access via mobile devices due to the rapid growth of tablets, laptops and smartphones.

Legacy security solutions often use technology that is static, providing little or no possibility for functional enhancement, or the ability to offer higher levels of data privacy. This inability to adapt also makes them easy targets for attack.

Often, legacy technologies are anchored to obsolete software, devices, protocols and products, making it difficult for the access control infrastructure to facilitate change.

Built on class-leading technologies, the latest access control systems ensure security is independent of hardware and media.

This makes it much easier for you to support new functionality and higher levels of data privacy.

The system also enables the use of many form factors as a credential, along with integrated functionality such as visitor management, time and attendance, cashless vending and more.

Upgrading your access control technology

If you continue to invest in outdated technology, you will never be able to progress to the technologically advanced access control solutions that provide enhanced data privacy management, convenience and functionality.

There are many reasons that upgrades might be avoided or delayed – these could include budget constraints, productivity impacts or workflow concerns.

However, delaying the change can have a negative and increased risk to your business, as technology obsolescence and escalating security threats can affect your ability to protect your people, facilities and assets.

The best approach is to be proactive and begin to replace older systems with new technology. This can be done gradually over time, and

ultimately results in a minimised risk of a serious breach in the future.

Access control solutions should enable you to adopt future capabilities without disrupting ongoing business operations.

While investment is required, there is the positive return in the form of improved security operations, more efficient workflows and/or reduced insurance premiums due to better risk management.

Taking steps to avoid a security event impacting the organization's workforce or data can prevent costly long-term legal challenges or negative brand and reputation effects which can take years to overcome.

Conclusion

Embracing the positive aspects of change requires an access control platform that meets today's requirements and is flexible enough to respond to future needs, all while meeting the highest levels of data privacy, user convenience and flexibility.

If you would like to find out how Impro Technologies can help you upgrade your existing system, please send us an email to

info@impro.net and we'll be in touch.

Alternatively, visit our web site and complete the form for a free consultation:

www.impro.net/upgrade.



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

HQ tel: +27 (31) 717 0700
Email: info@impro.net
Web: www.impro.net