Access Control 101.

ICT's ultimate beginner's guide to physical security.

Introduction.

Access control. What does that even mean?! Why do I need to know about terms such as intrusion or integrated security? Now you've got this guide, you'll learn the answers to all of this, and more.

It doesn't matter whether you're a business owner, a property manager, or an IT professional. Most people only tend to think of security once they have an issue. And that's OK, because you shouldn't have to worry about it all the time.

With a modern access control system, you'll get peace of mind, knowing that your staff or customers can stay safe – a key priority of any business owner or manager. You can also rest easy at night as you're less likely to get those annoying late-night phone calls because someone has forgotten to lock the door. And forget those costly call-out fees to change the locks every time someone loses a key.

Once you have a functioning security system, you won't even notice it. It just works.

But where to start? It can seem rather daunting – lots of acronyms, abbreviations, and technical terms that you've never heard before. We get it, we had to learn it all too. That's why we created this guide. Think of it as a fast track to security success. It's dotted with tips and tricks from our staff and customers to ensure you can make an informed decision.

So read on, learn, and emerge empowered to start your own access control journey, armed with all the knowledge you need to secure your premises.

What is access control?

Access control systems help a business to **minimize risk** and create a **safe environment**. The aim of access control is to manage entry so only people you choose (authorized users) can enter a property, or even specific areas within a building.

People you don't want (unauthorized users) are denied entry, and others, like visitors or contractors, get restricted access. All while providing an unobtrusive experience for approved people. A good access control system will also provide a layer of audit and reporting, should you need to track movements of people or goods around a site.

Why access control?

- Your site may have areas where you need to restrict and monitor who can enter
- You might also have health and safety requirements that mean you need to know where your team is at any given time
- You could run a 24/7 facility that needs to save power during downtime while still offering user access
- You have a gate that needs to open for the right people at the right time

You can meet all these needs, and much more, using access control.

When done well, access control systems should enable **effortless movement** and enhance the overall efficiencies of day-to-day business.

Evolution of access control.

Many businesses still use traditional locks and keys. Surprisingly, this technology has not progressed much since the 1860s when Linus Yale, Jr., patented his cylinder pin-tumbler lock. And yes, it's the same Yale you still see on some padlocks today!

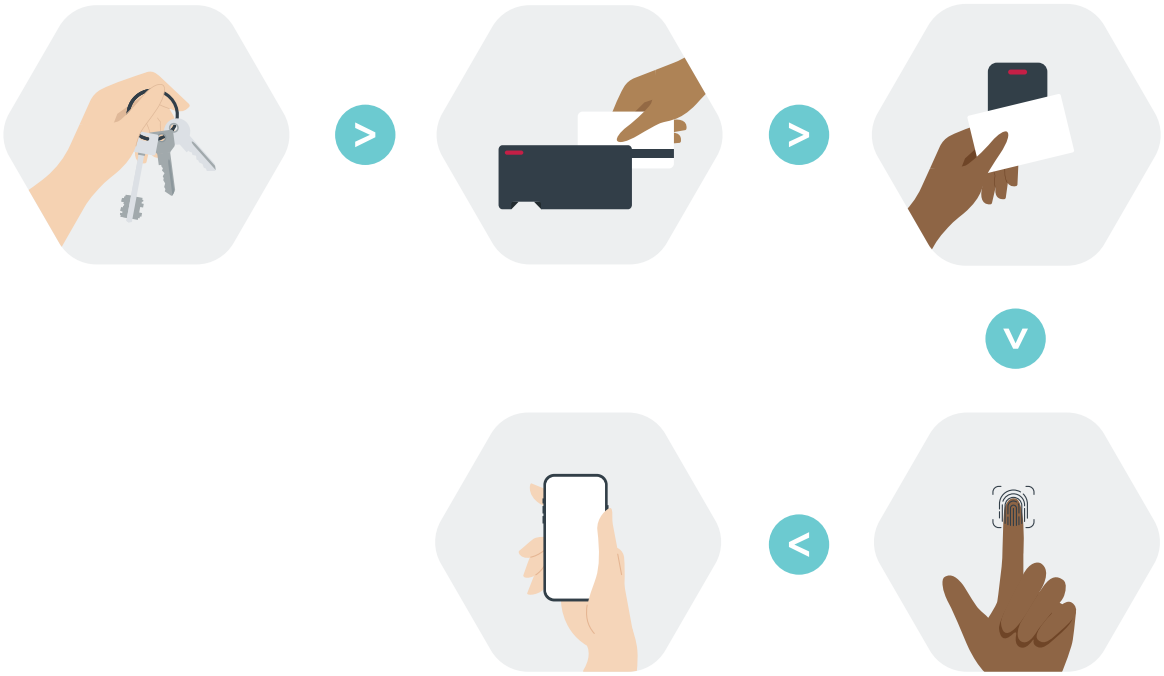
However safe traditional locks were, businesses spend a lot of time and money on locksmiths to rekey all the locks just because someone lost a key, and then giving new keys to everyone.

Technology has led to major changes in access control. Advancements in the 70s and 80s led to RFID card technology.

Then, the widespread adoption of the 125kHz proximity (or prox) card took security into the modern age. For a time, prox cards provided convenient and robust electronic access control.

As flaws in 125kHz became apparent, other technologies were developed - from PINs and biometrics, through to 13.56MHz proximity smart cards and mobile credentials - but until recently, none have looked to overtake the ubiquity of the humble 125kHz prox card.

However, the widespread adoption of smartphones and the Internet of Things (IoT) mean the next generation of security is being driven by increasing connectivity and ease of use.



The modern system.

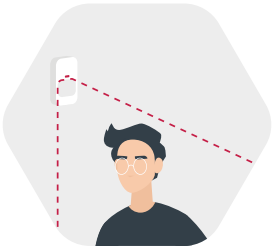
Modern access control systems give you the flexibility to make even small changes when you need them. If a card is lost, simply deactivate it and issue another without affecting anyone else's access. Easily change schedules to ensure security is not compromised on a public holiday or enable after-hours access for cleaners. You can even allow or disable access to certain areas on a temporary or permanent basis.

Ease of use is a crucial factor and removes a pain point for staff. Say goodbye to that clunky bunch of keys, and replace them with a single card, fob, or your mobile phone - which allows access to all authorized doors.

A modern system comes into its own when access is included as a part of an ecosystem that manages a site. When you combine access control with building automation and intrusion detection (such as alarms and video surveillance), multiple security products make your property even safer by working together.

Access control

Restrict entry and keep unwanted people out, but allow authorized users to enter.



Intrusion detection

Alarms, motion detectors, and video surveillance ensures that unauthorized access doesn't occur.

Building automation

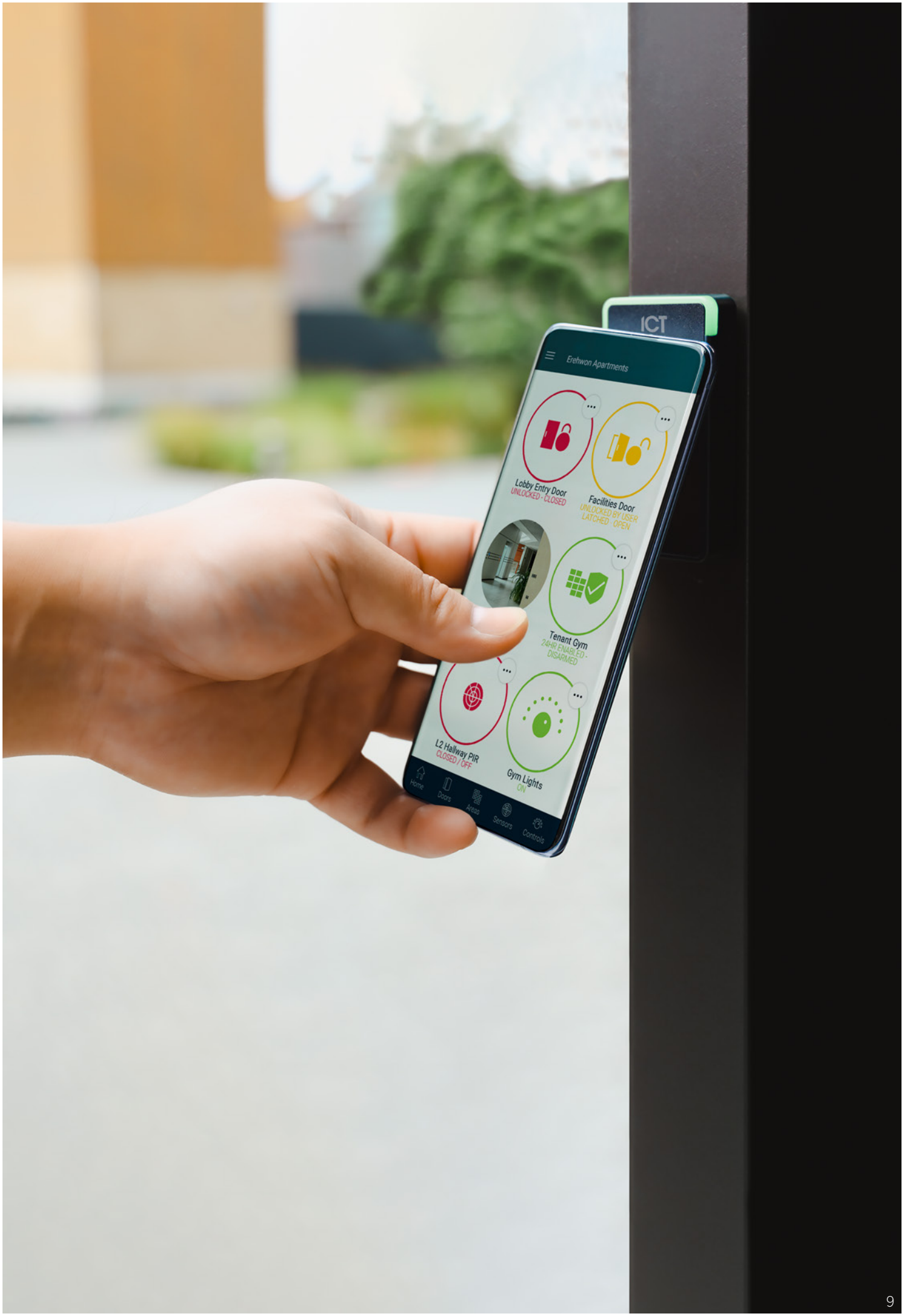
Reduce energy consumption by automating manual tasks such as turning lights or heating on and off.

A unified system means
you can control everything
from **one simple interface.**

Benefits.

- Increase in safety and security brings peace of mind
- Enhance employee satisfaction thanks to ease of use
- Save on replacement costs as your new system may work with some of your current security infrastructure (like motion sensors or cabling)
- Reduce false alarms that would be reported to monitoring services or authorities
- Incorporate added functionality into a single security system with third-party integrations (such as wireless locking, elevator controls, video surveillance)
- Gain extra cost savings and efficiencies by integrating with a Building Management System to reduce energy consumption by controlling HVAC (heating, ventilation, and air conditioning), lighting, and more
- The ability to sync data with external sources like HR systems or student management software so there's a single source of truth
- No more ongoing costs to rekey doors each time someone loses a key. Simply deactivate their card and issue a new one
- No after-hours trips when someone has left their key at home. Grant access or control the property remotely via web or phone
- Respond instantly to problems by setting up notifications to your mobile or monitoring service when an unusual event like a broken window or door being forced open is reported
- Future proof your business by choosing a modular system like ICT's that can scale with your business growth

> "The thing I like most is nothing ever goes wrong in the middle of the night like it used to."
>
> **- Tim Bealing, Environmental & Security Coordinator at Red Stag Timber.**


ICT
Erehwon Apartments
Lobby Entry Door
UNLOCKED - CLOSED
Facilities Door
UNLOCKED BY USER
LATCHED - OPEN
Tenant Gym
24HR ENABLED -
DISARMED
L2 Hallway PIR
CLOSED / OFF
Gym Lights
ON
Home
Doors
Areas
Sensors
Controls

The basics.

Parts of an access control system.

To most people, the only visible parts of a commercial access control system are the keycard that you swipe at the card reader to get in, or perhaps the keypad where you set the alarm. But there is a lot more that goes on behind the scenes to make a complete security system.

It all starts with a controller – **the heart of your system**. From here you can add different products depending on your business needs. A small business may just need one or two doors secured with a card reader for access and a keypad for an alarm. While a large organization may require many more features such as wireless locks, video surveillance, and elevator control.

Behind the enclosure.

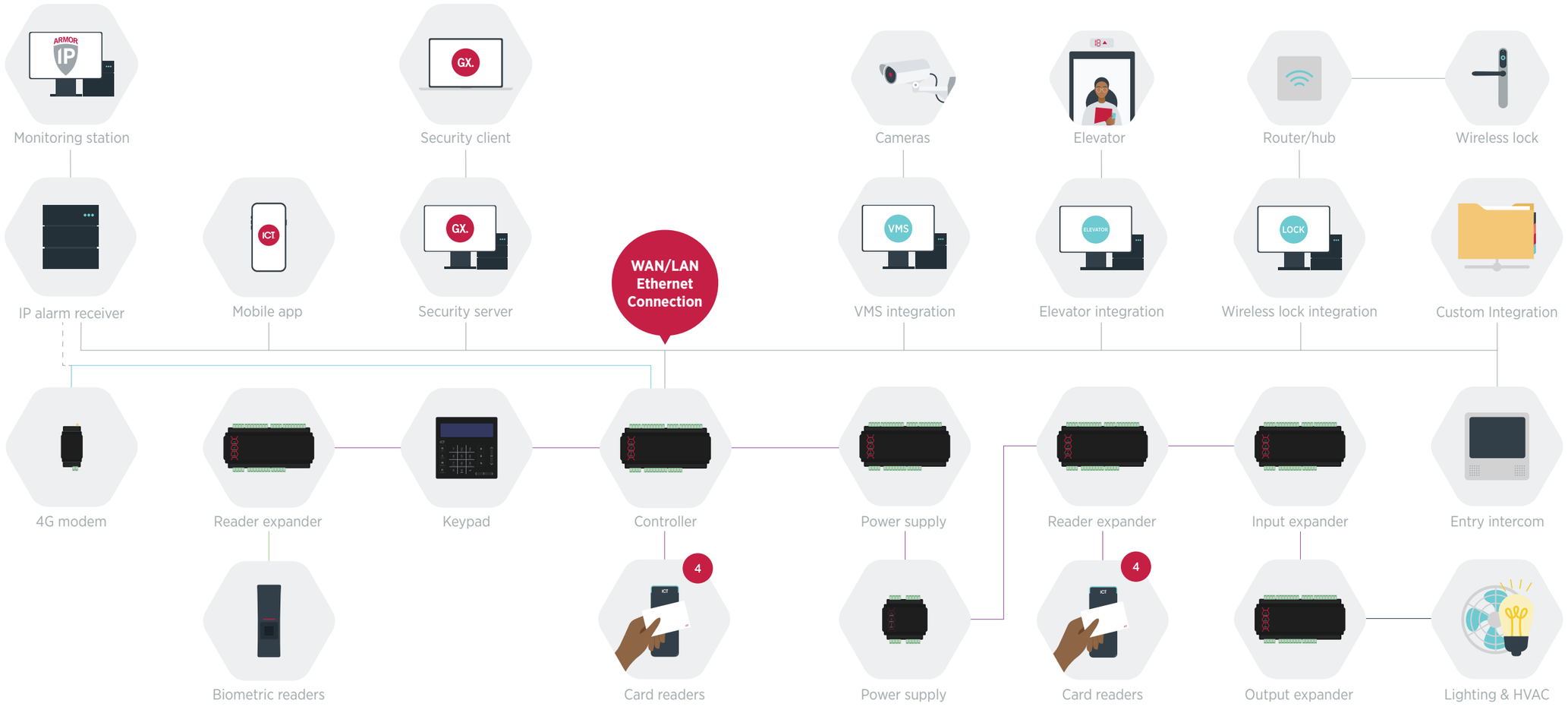
Overview and control of the system comes from your interface – which can be web-based, a mobile app, or standalone security client. Your access control software will have a status page (like a dashboard) which shows events generated by the system, and allows you to manage any security issues in real-time.

Security systems allow integrations with third-party products for added functionality, and secure transfer of data from external databases to automate tasks.

This could be onboarding new employees from a staff management system, or a visitor and contractor management solution.

Other security infrastructure you will see in access control systems are battery backups, wiring, electronic locks, and additions such as security cameras or passive infrared (PIR) motion detectors.

Put all these parts together and you can start to see how flexible (and potentially complex!) a modern access control system can be.



System requirements.

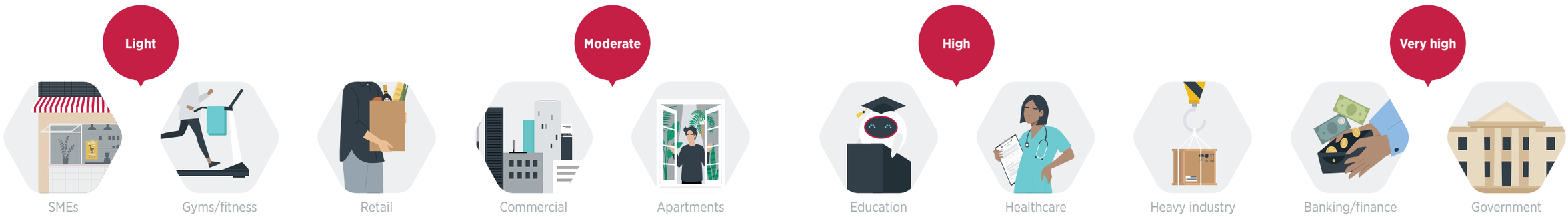
Access control systems are useful and effective whatever market your business is based in. As the diagram below illustrates, the security required can range from light to very high depending on the industry. While you'll find a lot of similarities in security solutions, some verticals may require specific features.

Basic features:

- Access control
- Alarms (intrusion detection)

Advanced features:

- Mobile solutions (access from your smartphone)
- Two-factor authentication (access card plus PIN)
- Third party integrations
- External database sync with API



Beyond the basics.

We have tried to keep it as simple as possible in this guide, but there are a few more concepts you should familiarize yourself with before you choose your system.

Understanding credentials.

A credential is what you present to the reader for validation. It could be a keycard, fob key, PIN code, mobile phone, or even your finger or face. The card reader checks your credential and validates it with the system before granting or denying access.

What you have

An access card or fob.

What you know

This could be a PIN or password.

Who you are

A biometric credential like a fingerprint or facial scan.

What you have makes up most credentials present in the marketplace today. This includes keycards, mag stripe cards, wristbands, key fobs, mobile credentials, and license plate recognition.

Credential technology.

As we mentioned earlier, not all credentials are created equal. Here's a quick rundown on the two most common card technologies.

125kHz proximity.

125khz proximity (or prox) cards are low frequency, and offer one-way data transfer that's unencrypted. They're fast and convenient, but **highly vulnerable.**

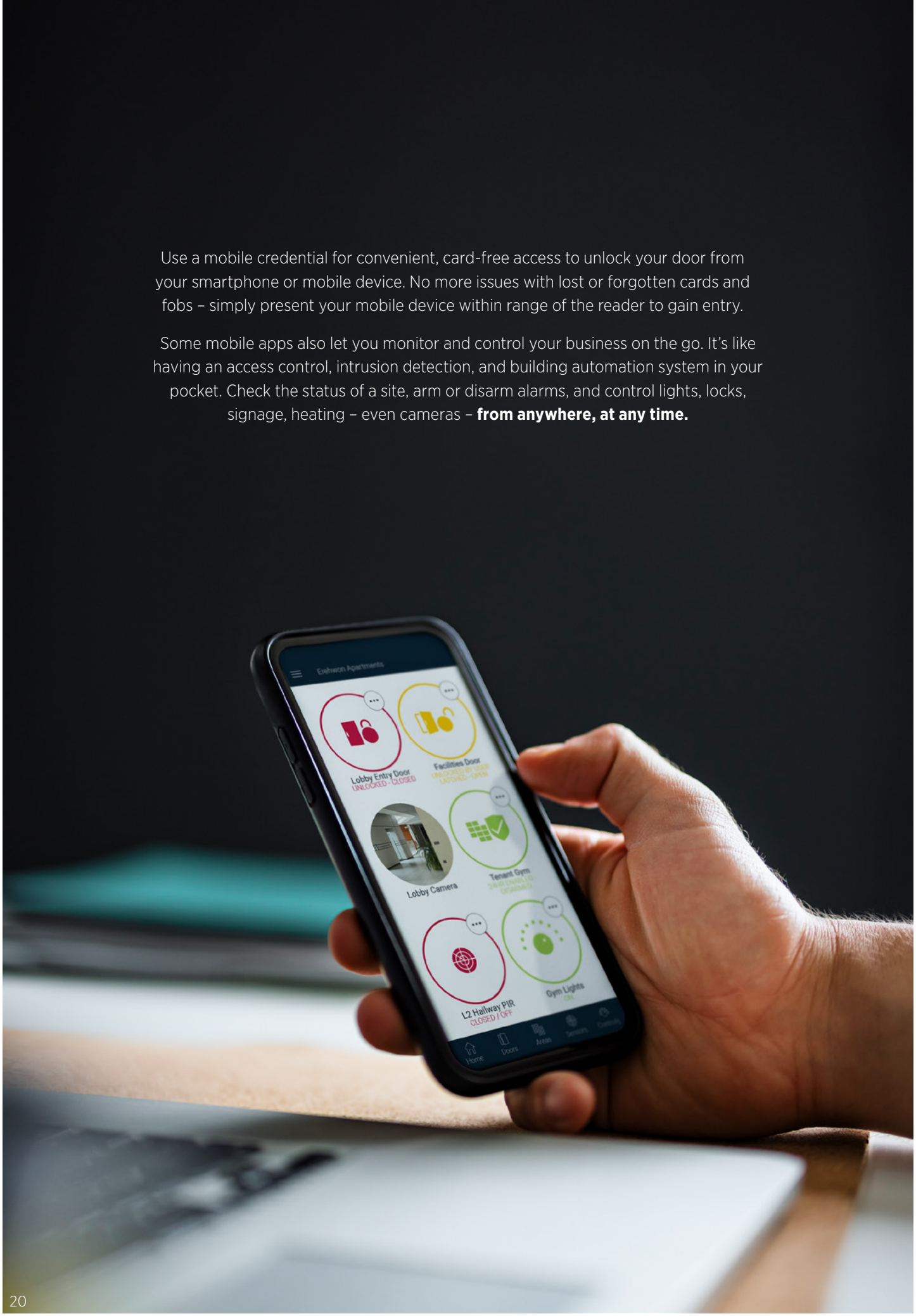
13.56MHz smart technology.

Smart cards are high frequency and allow two-way communication between the credential and the reader. They are encrypted and data can be stored on-board. Some formats even offer multi-sector functionality, so you can use the same card on a reader and wireless locks (or even to pay for public transport!).

For an industry-leading level of security, we recommend MIFARE DESFire for all sites. DESFire has the highest level of card security currently available so users can know that their credentials are protected by best practices.

Use a mobile credential for convenient, card-free access to unlock your door from your smartphone or mobile device. No more issues with lost or forgotten cards and fobs – simply present your mobile device within range of the reader to gain entry.

Some mobile apps also let you monitor and control your business on the go. It's like having an access control, intrusion detection, and building automation system in your pocket. Check the status of a site, arm or disarm alarms, and control lights, locks, signage, heating – even cameras – **from anywhere, at any time.**



Integrations.

Increase the functionality of your solution by integrating with third-party products. You'll add value to any existing technology and infrastructure investments, and truly unlock the full power of your system. Integrations can include:

- Video Management Systems (VMS)
- Wireless locking
- Wireless sensors & detectors
- Elevator systems
- Intercom systems
- Biometric systems
- Building Management Systems (BMS)
- Custom integrations

Video surveillance.

Detect problems early. If someone scans a stolen access credential, you can see on screen that they don't match the user. The security guard can deny access, then with perimeter camera you can track the potential intruder and send authorities a screenshot of their description and vehicle details.

Wireless locking.

Wire-free flexibility. When hardwiring locks isn't possible due to glass doors, other structural limitations, or even not wanting to run wires for aesthetic reasons – a wireless locking integration allows you to easily bring more doors online and reduce the number of physical keys required.

Custom integration tools.

Seamless solutions. In addition to the wide range of third-party integrations already available, you can use open protocols such as Application Programming Interfaces (APIs) or data sync to create a custom solution for your specific needs. This could be an automatic sync of information between an external database such as a human resources or student management system and your access control. Or using an API to enable functions like control and management of access and lighting/building automation in third-party app or software.

The 5-step method for access control.

The purpose of access control is to secure your premises so that unauthorized people cannot walk in off the street. There is a five-step method that acts as a pathway to ensure the correct process is being followed. By following this path, you can be sure that you'll have a robust system in place to protect your business.

Authorize

The process of changing a stranger to someone known to your organization. Once authorized, you will likely use RBAC to assign their privileges.

Authenticate

When a user presents their credential to the reader for authentication, the system decides whether to grant access.

Access

If authenticated, access is granted and your door unlocks for entry.

Manage

Administrators can track activity and manage changes including adding new staff and updating area permissions.

Audit

Some organizations have specific legal compliance requirements for auditing. But, it's also good practice to ensure that your system is working and create a baseline to help track suspicious activity.


ICT

Choosing your system.

As you can see, there are many things to consider when thinking about an access control system.

> The fundamental thing to think about is what is the purpose of the security system? Ask yourself what security perception are you trying to portray? A highly secure premises with multiple security layers like gates, access doors and turnstiles, or an open and welcoming space with restricted areas?
>
> **- Chris Newton – Head of Project Design at Focus Digital Security Systems.**

Now, take a moment to think about potential risks such as the safety of your staff and customers, theft, or even spying. Decide which of these risks are most important to address and how thoroughly you need to manage them. Also, make sure to check if there are any specific insurance requirements you need to meet.

Our experts can guide you through this process, but there are some questions to ask yourself before you begin:

- How many doors would you like to secure, and how secure do these areas need to be? Will people need a card to get out as well as in, or just push a button to exit? And will any doors require both a card and PIN? This will determine the number and type of card readers you'll need
- If it's a retrofit, what do you already have? You may be able to save money by using existing hardware such as motion sensors or card readers with your new system and save costs
- Would you prefer to use a mobile credential on your smartphone, a physical card/fob, or even fingerprint or facescanning biometrics?
- Does the system need to integrate with a new or existing CCTV surveillance system?
- Is there potential to automate things like lighting and air-conditioning to reduce energy consumption and operating costs?
- What industry does your business fall under? And is there anything that you do differently that we should know about?

All this information will help a security expert tailor the system to your unique needs.

It's important to understand that not all access control systems will give you all this flexibility. An ICT Protege system brings together all elements of access control, alarms, and automation into a single unified solution, adding value to the infrastructure your business already has.

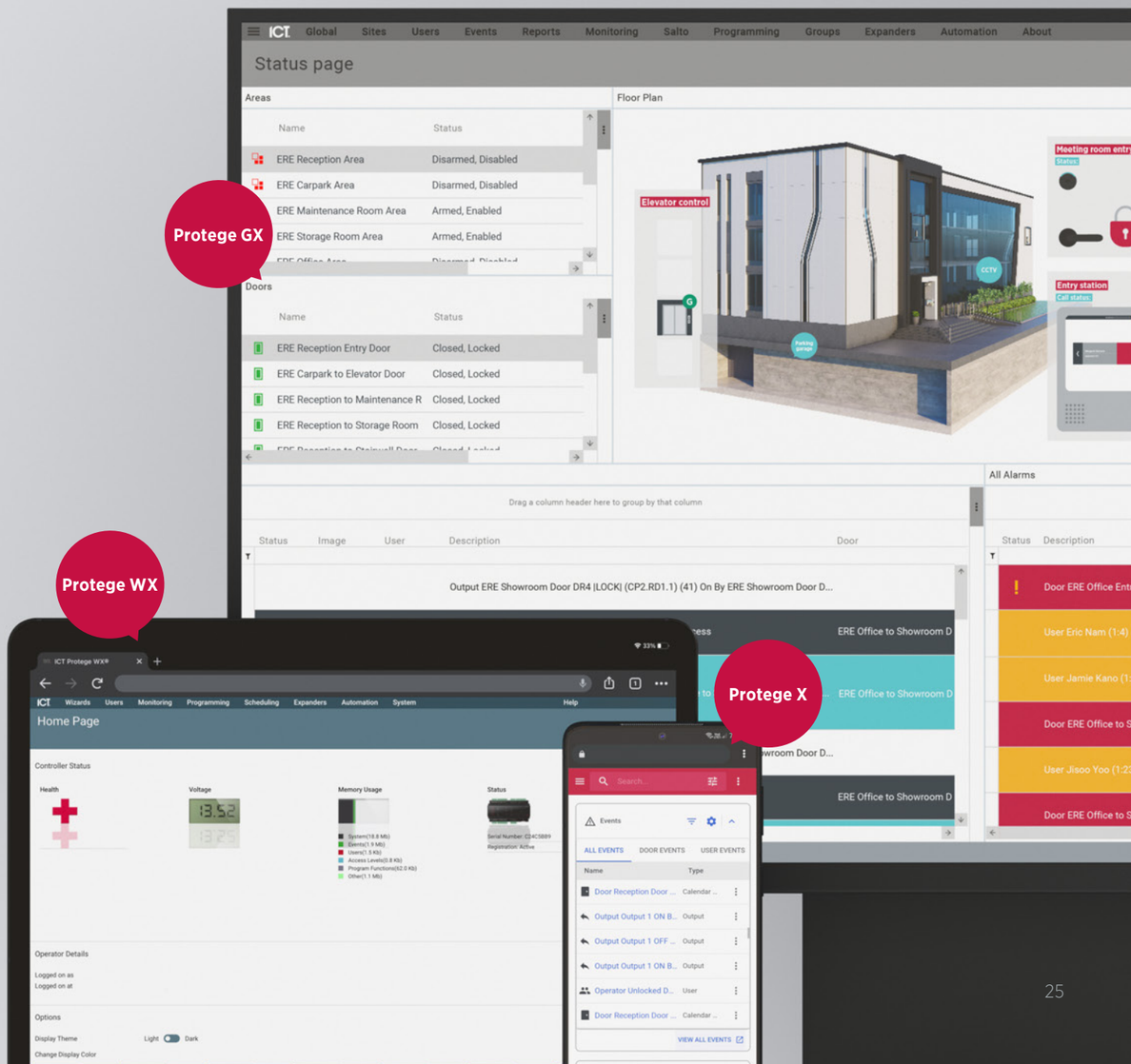
ICT system options.

Small to medium businesses.

If you have a small or medium business that you'd like to secure with the minimum of fuss, you can get access, alarms, and so much more with **Protege WX**. For businesses with multiple sites, you should consider a cloud-based platform like **Protege X** that can scale as you do.

Large enterprise organizations.

Get a feature set that's easy to operate, simple to integrate, and effortless to extend. A comprehensive solution like **Protege GX** future-proofs your security and provides true benefits to any organization.



Next steps.

Now you have read Access Control 101 – ICT's Ultimate Beginner's Guide to Physical Security, you should understand the basics involved in securing a location using a modern access control system.

With an understanding of the terms you might hear, questions you're likely to be asked, and the benefits provided by an integrated security platform like ICT's Protege WX, Protege X, or Protege GX, you can now move forward with confidence.

Talk to one of our experts today. They can put you in touch with one of our qualified installation partners in your location, so you can take the next step in your security journey and provide peace of mind that your most valuable assets – your people and your property – are secure.

About ICT.

Founded in 2003 by Hayden and Rachael Burr, ICT began with a focused vision to provide innovative and easy-to-use electronic access control and security solutions. Almost 20 years later, tens of thousands of companies worldwide use ICT products and systems every day, and our vision remains steadfast and engrained in all we do.

With headquarters in Auckland, New Zealand, we have a global presence and an international reach. Our offices in USA, Canada, Australia, UK, Dubai, and Hong Kong provide full local sales, support and service to our clients and partners around the world.

Innovation is in our DNA.

With more than 40% of our staff dedicated to research and development, innovation is a core part of the ICT DNA. When you invest in an ICT solution, you can rest assured that your investment is protected by the best in the industry.

From design to dispatch.

Every ICT product is designed and manufactured in New Zealand from our state-of-the-art purpose-built premises, with 100% of products going through rigorous testing standards to ensure superior quality.

One solution, maximum value.

Our use of open technology allows our products to integrate seamlessly with your existing systems, providing a comprehensive solution that adds value to the infrastructure investments you already have on site.

This is all backed up by local sales, support, and training. In addition, we offer a 5-year warranty for our ICT Dealer Network members, providing the perfect solution for your next project,regardless of scope.

> “Working with ICT has been an exceptional experience. ICT’s well thought through modular design meant we could deliver the project on time, on budget, and to the full satisfaction of our client.”
>
> **- Mark Stytsenko, Technical Director at DockCom.**

Designers and manufacturers of integrated electronic access control, security and automation products. Designed & manufactured by Integrated Control Technology Ltd.

www.ict.co