THE MUST-HAVE ACCESS CONTROL CHECKLIST FOR PROPERTY MANAGERS

Property managers are tasked not only with managing the day-to-day operations of the real estate they oversee, they're also challenged with safeguarding and securing it. That's a lot to think about, as there are many variables to consider. And, those variables are often contingent upon the real estate itself.

The measures needed to secure a property almost always depend upon its location, risk level, hours of operation and other vulnerabilities specific to the property. By taking inventory of these factors inherent to their particular property, managers can effectively pinpoint the best combination of security measures to implement. Among the most important are usually:

intrusion and fire alarms · video surveillance · visitor management systems · and, topping the list, access control.

Controlling who should– and who should not – gain entry into a property typically ranks as the most pressing concern for a property/building manager. Having an unreliable access control system is enough to keep a Property Manager up at night, which is why access control leads the list as the most crucial component of a security strategy.

There's a lot to consider arriving at that strategy. Such as deciding on which system will be the most effective and reliable, selecting a security dealer or integrator to properly install it, and managing its ongoing operation and respond to emergency access control breach situations. The Catch 22, unfortunately, is that, while Property Managers know what should be done, they're not typically the best person to execute. Property Managers, after all, are not necessarily security experts. Many simply aren't equipped with the expertise needed to choose and invest in an access control system best suited to their property and its residents.

If you're a Property Manager, and this strikes a chord, read on. We at Kastle Systems, the leader in managed security, are here to help. We are dedicated to guiding and advising you on all aspects of your physical security program and have put together a few access control pointers to help you along the way.

The first step is:

DESIGN:

Every building or space that's constructed is built with a future-proof design in mind. Your access control choices should do the same. Keep in mind, that because access control products and systems are developed to address specific security concerns, it's important to first define who you are protecting, and what you're protecting them from, before selecting a product, vendor or methodology. That way, you can determine the system parameters that best meet your needs and those of your tenants.

These are the types of questions you should consider:

+ How many points of public access are there? Should each public access point assume the same level of access and restriction?
+ Which solution would best suit your property and tenants – a stand-alone keypad, a self-contained system or one that's integrated with a complete access control system?
+ How will the system be monitored? Will you have a dedicated staff with a designated work space on site or would it be more efficient and/or cost effective to outsource to a third party monitoring company?
+ What will the plan and policy be with regard to tenant occupancy turnover? It is typically the Property Manager's responsibility to collect all the issued key cards from vacating tenants.
+ Give some thought to the level of encryption the access credentials will need to ensure the property is safeguarded. Standard 125 kHz Prox card technology is widely used and affordable but it can be easily hacked. Card credentials also require that the Property Manager keeps an up-to-date account of all cards in and out of use. New cloud-based systems working with mobile-device enabled credentials are another option and growing in popularity and adoption.
+ Are you confident you can adequately answer these critical questions, or would it be prudent to turn to an expert for assistance?

There is a long list of considerations to think through before you determine the functionality of your access control. But before making any recommendations, let's move on to **step two**.

INTEGRATE:

Whether you're inheriting a pre-existing access control system or starting from scratch, it's important to consider how all the components of your solution will work together. Property Managers often struggle with how best to integrate their building's security technology with individual tenant's technology.

To help ensure your systems work in unison, keep these questions in mind and don't be afraid to pose them to your vendors:

+ Can the shell-building system accommodate potentially different individual tenant access control technologies for their spaces?
+ How integrated should the access control system be with identity management or with video surveillance?
+ Can the integration be used to trigger automated tasks like attendance and recording?
+ Will access activity be recorded electronically, and, if so, how will the data be stored and backed-up?
+ Do you need an open application programming interface (API)? While many providers boast an open API, which makes integration with other technology possible, they don't always share enough data points to allow for an effective integration. Be sure to explore this with the security vendor(s) you vet.
+ Flexibility is key. Does your solution need to enable mobile access that can grant or deny entry across multiple spaces?

FUTURE-PROOF:

Access control technology involves sophisticated equipment and complex software that needs to be regularly updated as developers make upgrades and improvements. To help ensure your business stays secure, it's important that your system is "future-proof" – that it continues to work the way you want for the lifetime of your building. Coordinate ahead of installation to determine how will it be monitored and updated.

MANAGE & MAINTAIN:

Once you've made these educated decisions and decided on a well-designed system from a top-notch access control vendor, most of the actual access control user experience has yet to occur. The day-to-day monitoring, management and maintenance of your access control is just as important to consider as the system you purchase.

Keep these points in mind:

+ Who will monitor the system? What are your staffing needs, the hours of operation and the backup contingencies, should issues such as a power outage, arise?
+ Will the access control vendor host in-person, on-site training for your staff? Will they return for new staff training in the future? Do they charge for ongoing training?
+ What maintenance or service agreements will be put in place for your access control systems?
+ Will the access control software be periodically updated and who is responsible for timely updates – your staff, the manufacturer or service/security integrator vendor?
+ If your security procedures change, who will help you reassess the access control plan for gaps?

It's critically important to choose a security provider that does more than install access control hardware and software, but also acts as a strategic partner to help ensure your system stays at optimal performance long after the initial installation.

There is much to consider when implementing security for your asset. If you're feeling overwhelmed by all the possibilities, give us a call. We'll be happy to walk your space and provide a complimentary assessment to help you determine the best long-term solution for you, your staff and your property.

Click here for more information on access control for property managers.