Access Control System Purchasing Guide

Introduction to the Access Control System Buying Process

What's inside:

- Trends & Types
- Software
- Credentials & Readers
- Features
- Questions to Ask a Dealer

Creating the perfect access control system requires careful assessment to ensure the proper levels of security. Start by analyzing your individual needs. This includes any regulatory restrictions you may be subject to. With all aspects of your business accounted for, you can design the system in the most effective manner, making it as cost-effective as it is functional.

Businesses seek to install Access Control Systems for a variety of reasons, including:

- Safeguard data
- Secure goods and raw materials
- Protect sensitive equipment
- Restrict access to "clean rooms"
- Restrict access to back up servers

In designing a risk management framework (RMF) and accessibility hierarchy, your businesses will be able to identify an appropriate access control system. Typically, businesses delegate this task to a Risk Management Assessment Team. The purpose of this team is to assess and recommend the best design for an access control system.

Security levels

Different areas of a business may require different types of access control. Access control systems may include a combination of the following components:

- Access cards
- Card readers
- Keypads
- Locking hardware

A good example of this would be a construction company. Keeping its heavy equipment under locking hardware would be the perfect solution to discourage theft and vandalism. However, unless the on-site construction trailer is storing smaller equipment, a simple key lock may be all that is necessary.

An example of a very simple controlled access system is utilized at storage facilities. A code or card is provided to the renter of a storage unit. Once inside, it is up to the individual renter to provide additional security to their property – the responsibility is on them to protect their assets.

An example of a business that requires a sophisticated access control system would be a financial institution. More than likely, they would utilize every type of access control device throughout different areas of the operation. For example:

- Employees would be required to utilize keypads for access to the main premises
- When entering a vault, they would be required to swipe their access cards in a card reader to enter locking hardware
- Accessibility is further restricted to certain areas based on security clearance
- Elevators can be restricted to certain floors, also based on security clearance

Designing the most effective access control system takes some planning. Too much security and the system can become cumbersome and people will get lax about using it. Too little security and you risk losses.

Purchasing considerations

Purchase considerations for an access control system have a large impact on the planning phase of your system. While each access control setup will reflect the security needs of your company, there are three major aspects common among all:

- **System integration**: When planning an access control system, make sure you take all other systems that may be compatible into account. For example, you may decide to incorporate control of your video surveillance, alarm systems, security doors, and even the elevators. By combining these into a single platform, you can cut costs on the number of staff required to monitor each system and make their responsiveness faster and more cost-effective overall.

- **Expandability**: Your security needs will change over time. Whether you need to add additional users, checkpoints, rooms, or entire buildings, the ideal system will offer a quick, straightforward option for building in new items, as well as eliminating those that are no longer applicable.

- **Requirements and codes**: All systems must adhere to guidelines enforced by the National Fire Protection Association (NFPA), detailed in NFPA 101: Life Safety Code. Have a representative from the NFPA review the system design for your access control

system, as well as any local legislative bodies that oversee aspects of construction such as city planning or engineering departments.

Individual design elements you'll want to consider include:

- **Door configuration**: Do you need badges/ID readers, electronic locks, contact alarms, and/or 'request to exit'?

- **Systems availability**: Will you monitor and access the system through a localized, hardwired terminal or mobile, web-enabled devices?

- **Fail-safe or fail-secure**: Does your facility require 'safe' locks that unlock all doors during a power outage or 'secure' locks that keep doors locked? Note: there are numerous instances where fail-safe locks are required by fire and life-safety codes. Check with your dealer for any additional questions on compliance.

- **Standalone access or networked control**: Do you need to control a single door (with limited options) or an entire system that's interconnected throughout your facility?

- **Software licensing**: This may cover user access and ongoing service contracts for system software platform.

Trends

As with any process that incorporates technology, access control systems are continuously in flux. Before you settle on a particular type of system, take a few minutes to review the following trends – in particular, how they may impact the integration of video surveillance, alarms, and similar business efficiency systems.

Wired vs. wireless

This is one of the most common debates among almost every technology that facilitates some form of communication. As with other processes, the decision will largely be determined by the size of your facility.

Smaller operations such as single-floor office plans, retail shops, and other small businesses with anywhere from 1,000 to 1,500 square feet may be able to make use of wireless components. Larger organizations with multiple floors, buildings, or even separate geographic locations will find their range too limited to be of much use.

Here's how the two compare:

Wired

Most access control systems use electrified strikes and locks, often including magnetized locks. Connected to a centralized power source, this enables you to link an expansive area that encompasses multiple zones, floors, and buildings into a single system.

This setup provides a number of advantages. The first is that it allows for the remote monitoring and control of all doors within the system, enabling staff to secure an area or provide access with the simple push of a button.

In addition, a wider selection of wired components tends to be more readily available, free of the frequently upgraded compatibility issues that can hamper wireless setups. Finally, the signal is almost guaranteed to be quick and uninterrupted in a wired setup, providing reliable data transfer, whether it's from a door alarm, intercom, or integrated video feed.

The main disadvantage of a wired setup is cost, especially if it's retrofitted into an existing structure. The cost of running cable is one of the main expenses, both initially and if any repairs are needed. Tying all the wires together in a box is another specialized service and one that adds to the cost. Additionally, there are cases where a wired setup is either problematic, elevators being one example, or practically forbidden, such as buildings with asbestos.

Wireless

Wireless access control systems can't provide the same distance a wired setup can. But what they lack in range they make up for in other ways. The first is that they can be installed in areas that are too costly or unavailable for retrofitting. Some commercial properties are burdened with endless streams of red tape when they want to make physical changes to their location.

Common examples include small businesses, medical services, and professional offices that lease space within a strip mall or office building. In these instances, wireless access control systems can provide a comparable level of service and avoid the regulation associated with tearing up walls, floor, or ceiling.

Another benefit to a wireless system is that it can be extremely cost-effective when compared to a wired installation, dramatically improving the ROI in some instances. Not only will you save money by eliminating the need to run wire for power and component connectivity, you cut installation costs as many wireless components can reportedly be installed in 45 minutes or less.

In fact, it's this savings on labor that often represents the biggest difference in cost, with wireless installations costing nearly 30% less than their wired counterparts. It's worth noting

that the cost on the parts themselves were pretty much even (the higher price tag on wireless technology makes up for the purchase of the wire).

The main disadvantage of a wireless access control system is the cost of maintenance. Like any computer, the software platform and the components themselves require a steady stream of platform and driver updates. On a small system with a handful of components, this usually isn't a big deal. But with larger installations, reliable IT support – either in-house or purchased through the dealer – are a must.

Integration

With more and more businesses using a variety of efficiency systems to cut costs and improve their responsiveness and overall service, system integration is often top-of-mind for those purchasing an access control system. In particular, many buyers and business owners want it to be compatible with two specific functions:

- **Human resources**: If you're a small business with less than a few dozen employees, HR integration probably won't mean much to you. But if you oversee an organization that has hundreds or thousands of employees, your turnover demands the real-time integration of access control and HR. Primary concerns include termination and suspension, but other companies may use it to align with scheduling, limiting access based on shifts and vacation time. This feature can also be used to control departmental changes, granting or rescinding access to databases, filing cabinets, storage facilities, parking structures, and entire buildings.

- **Security**: Similar to the integration with HR, combining your access control system with security can immediate eliminate any questions of access for employees and guests. It also cuts down on the amount of labor required by security personnel. Each individual has been pre-configured in the system. All that remains for security staff to do is issue or verify credentials, freeing them from the lengthy process of data entry and liaising with other departments (often including HR).

Types

The ideal access control system balances competing demands for security and convenience. Within its framework, a myriad of add-ons, upgrades, and options exist, allowing you to customize the system to fit your exact needs. As you begin to compare access control setups, you'll notice there are four basic frameworks or types:

1. Networked systems
2. Standalone systems
3. Free exit systems

4. Control exit systems

Think of these as packages that can be tailored to fit. With that in mind, here's how they compare.

Standalone access control systems

Standalone systems manage security for a single door, area, or location. For example, they may be used to secure a front door, back door, interior door, or warehouse door within a facility. Common applications include receiving doors, cash rooms, and interior offices that require limits to public access. Each standalone access control system operates independently of all other systems (thus the name) and is limited in the level of control it provides.

Standalone access control units are not scalable. So when opting for a standalone system, it's essential to consider use and location:

- Are your access control needs limited to a single entry point?
- Is the door or area visible and easily monitored?
- Will your access requirements change over time?

This type of solution typically works best for smaller businesses. Examples include doctors' offices, auto repair shops, and similar locations that have staff positioned within sightline of the access control door. In addition, these locations don't anticipate growth related to the size of deliveries they receive, an issue that would require a larger door or additional entry points.

Costs related to a standalone system include the following components:

- Cabinet Locks - $1,022
- Keypad & card combos - $329
- "Buzz-In" kits - $438
- Keypad - $199
- Memory stick access - $729
- Proximity cards - $1,370

Networked access control systems

Networked access control units allow you to oversee security at several vantage points. This type of system is notable for the wide range of convenience and portability it provides. Common components include IP cameras or some type of intercom system as well as door-mounted ID readers. This allows personnel to identify and track both employees and guests. Many systems can also be designed to be Bluetooth compatible, allowing individuals to use their mobile devices as ID to gain entry.

The real benefit of networked access control is that it's run through software that allows you to manage the entire system from any web-enabled device, including many tablets and smartphones.

Other benefits include:

- Programmable schedules
- Managed via standard web browser
- Comprehensive reporting, including people, cards, events, special days, schedules
- Data exportable into XML file
- Prevent unauthorized visitor access
- Accommodate trusted vendors and suppliers
- Generate traffic reports

This type of an access control system is designed for companies that oversee multiple buildings, possibly in different geographic locations. Warehouses, schools, and similar organizations with a large footprint typically benefit the most from this type of access control. But the web-based application delivers benefits and business insight to business owners and organizations at every level.

That's because networked access control systems provide excellent metrics. They can be programmed to track entry/exit times by employee or department. The system can perform centralized lockdown in the event of an emergency security threat. They can also provide an extra layer of security for protecting people, assets, and facilities.

Costs related to networked access control systems include the following components:

- IP cameras/Intercoms - $430 to $790
- Keypad & card combos - $200 to $330
- Bluetooth sensor - $280
- Software - $840 to $5,100 (depending on licenses included)

Free exit systems

Free exit systems make exiting a secured room or area quick and easy, removing all requirements for leaving the area. Simplifying movement for employees and visitors alike, the system typically uses one of two methods to activate the door, a motion sensor that opens the door when someone approaches, or a hand-activated button or crash bar.

Several types of free exit systems exist, meeting every conceivable application. They include customizations for commercial enterprises such as storage unit facilities, apartment buildings, manufacturing facilities, underground parking, and high-rise business complexes.

While a free exit system facilitates leaving an area, it can also be used to control that location in a number of ways, including:

- On-site attendant
- Magnetic cards
- Remote attendant
- Keypads
- Digital code transmitters
- Biometrics

Swing gates represent another type of free exit system. Commonly used by subdivisions, gated residential communities, apartment complexes, and businesses, they're available in a variety of materials including cedar, wrought iron, and vinyl. Cost is impacted by the size of gates you install as well the number of cameras, telephone systems, or radio controls integrated into the system. Specific types include:

- Swing arms
- Swing gates (single swing and dual swing)
- Rolling gates (single slide and dual slide)

The total cost of the system will be determined by the type of access/exit point you wish to install. For example, you may have multi-lane access and single-lane exit points, or vice versa. Many operations incorporate several different types of access/exit systems within their facility. While some may choose unattended gates, access to the actual facility may require another form of access control system.

Costs related to a free exit access control system include the following components:

- Exit wands $57 to 85
- Control boards $75 to $80
- Gate controls $10 to $400
- Keypads $50 to $265
- Warning devices $50 to $450
- Solar panels $125 to $675

Control exit systems

Exit control systems do exactly as the name indicates – they prevent unauthorized exit from a secured room or location. Typically using magnetic locks, an exit control system switches to a locked state and remains locked if an alarm is triggered.

Hospitals frequently use exit control locks to prevent the removal of newborn babies and children beyond authorized boundaries. Airports are another prime example. Many of them are equipped with exit control systems within quarantine facilities as well as customs clearing areas.

An additional type of controlled exit system is similar to a free exit setup but includes a delayed release on the lock. These delayed exit point locks may be incorporated into fire doors in an office or retail setting and are frequently built into memory care hospitals and retirement centers to prevent individuals from wandering away from safety. The only time these units operate as free exit is during a fire alarm or power failure.

A third type of exit control system is known as "request-to-exit." It includes a pushbutton that opens the door, such as those provided for wheelchair-bound individuals. Depending on the needs of your business, authentication methods including card readers or biometric identification may also be used for both entry and exit in this type of system, controlling employees, guests, and unauthorized individuals.

Complete systems can run from a few hundred dollars to tens of thousands depending on the components and level of security it provides. Specific costs related to a controlled exit system include the following components:

- Locks - $150 to $660
- Alarms - $280 to $300
- Crash bar - $320 to $350
- Exit pushbutton - $91 to $100
- Turnstile hi-gate - $6,500 to $11,900

Software Types

There is a software system for every type of business. Combining a variety of card readers and door controllers, access control system software is flexible and cost-effective. From college dorms and small businesses to government agencies and national conglomerates, you can design the perfect access control system with the right software. These systems are user-friendly with a host of features that increase security and contribute to productivity.

Whether you need a simple badge system to open doors or one that includes surveillance, alarm management, and other controls you can design the perfect access control management system through a variety of software types. Access control software allows you to create the best security management system as well as integrate a variety of security equipment.

Some of the benefits of the software include:

- Microsoft Office layouts, providing user familiarity
- Systems are scalable
- Role-based permissions
- Mobile apps are available
- Multi-location configuration
- Need-to-know restrictions
- Routine security/administration tasks can be scheduled
- Add-on language packs available

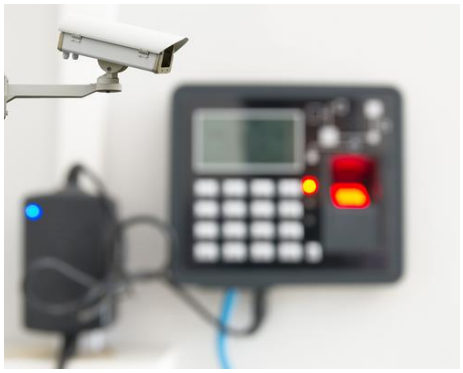
Software types come in four basic configurations:

1. Managed Access Control (MAC)
2. Role Based Access Control
3. Discretionary Access Control
4. Rule Based Access Control

Managed Access Control (MAC)

Managed access control combines the technology of access control with the added security of live personnel. In a MAC environment, a security professional is always present, providing a set of eyes on all avenues of entry and exit. It's a system that proves beneficial in many aspects. For example, a security guard can monitor everyone who approaches a secured area, observing unusual behavior that a camera may not "see."

This type of software is often integrated into access control systems by companies that opt for third-party security personnel, like those provided through a monitoring service or security company. A MAC platform also commonly replaces keyed locks with badge- or fob-based identification that enables a system manager to pre-program the dates and times a specific individual is allowed to enter, further simplifying building security.



Role Based Access Control (RBAC)

Role-based access control systems allow managers or HR to assign specific levels of access to every individual that enters a building, from employees and support personnel to guests. Individuals are granted access based on their individual roles and responsibilities. In the event these designated individuals are absent, access may be restricted until a person of equal or greater authority can be located to perform the necessary functions.

RBAC is highly specific, not necessarily granting lower levels of access to an individual simply because their current level meets or exceeds it. In this way, it allows an organization to customize the access of a specific role and further tailor individual access to those who perform more than one role. Given the administrative freedom it provides, RBAC tends to work well for companies that have a high rate of turnover.

Discretionary Access Control (DAC)

A discretionary access control system provides access to employees, sub-contractors, and guests on a flexible and sometimes temporary basis. Unlike a role based software model that tends to manage groups of individuals en masse, this type is usually defined on an individual level, often limiting which resources an individual has access to.

This software is designed to restrict objects, files, or areas. Based on the individual rights assigned, individuals with higher access authority may be able to assign permissions to others at their discretion.

Rule Based Access Control

Often referred to as automated provisioning, this type of access control is strictly based on predetermined rules that are assigned to individuals. Common examples include rules based on date and time, role, or function within the organization. They can even be used to restrict or allow an originating IP address. Once an event is triggered, such as an individual attempting to access certain areas of your facility or files on a computer, the events are compared to the access rights. If there is a match, access is permitted.

Rule based access control is also used within a system to restrict the specific actions an individual can take once they have access. This can be used to limit access to secured areas within a larger room as well as prevent the unauthorized copying of computer files or hardcopy data.

Common features

All four types offer flexibility in setting up and monitoring access and exit points within each area of your company. Regardless of the system you choose, the software should allow for the following setup and configurations:

- Easy integration with HR systems
- Access restricted and configured by date ranges, specific days or specific times
- Easy to configure access rights, by individual, group, card type or badge type
- Contractors can be set up according to the accessibility times you designate
- Ability to encode smart cards
- Special advanced features are available, i.e. extended door unlock times for individuals with disabilities
- Easy to configure accessibility within a multi-tenant or more complex environment
- Visitor management system

Pricing

As they include relatively similar features, many of the software packages run within comparable price ranges. Expect to pay $100 to $250 for a basic platform that manages access control through PIN codes; $420 to $1,000 (and up) for mid-range solutions that offer RFID access control for up to 30,000 users; and $2,000 or more for comprehensive access control software suites that provide the full range of customization and tracking as well as web and/or mobile compatibility.

Credentials & Readers

There are several types of card controlled access systems available. Depending on the level of security your business needs, accessibility can be restricted via the use of these applications. Cards can be programmed to provide access based on the four software types mentioned above.

Below, we cover popular credential and reader options.

Card controlled access systems

Card control access systems include:

- **Key card access / proximity cards** – These systems utilize swipe cards or RF cards that activate within a certain distance of a reader. One of the more common forms of employee identification, they can be clipped to a belt or necklace and are embedded with a metallic coil that stores identification data. Similar to a credit card reader (though they do not require a "swipe"), data is passed to the system when the card interacts with the reader, granting access based on the data specific to that individual.

- **Automotive cards (for garage access)** – Similar to garage door openers, these cards are placed within a vehicle and communicate through RF for access or exit points. The difference is that no one has to push a button. It's not uncommon to find readers that can grab the data off an automotive card from up to six feet away. This not only simplifies access for the driver, it also expedites vehicles through a security checkpoint. It's worth noting that this type of setup is not typically used by organizations requiring a high level of security as it provides automatic access to anyone possessing an active automotive card.

- **Magnetic stripes or barcode** – A close cousin to key card access, magnetic stripes can be incorporated into a variety of personal identifiers, including keycards, badges, and fobs. They can provide access for a single purpose or a variety of different uses, often double-coded for building security and garage access as well as cafeterias and departmental billing codes.

Access rights can be assigned to meet the needs of the entity. High-rise buildings may utilize key card access for garage access as well as access to the building or elevators with the same key card. Conversely, a keypad may be utilized in an elevator or on a secured door for added security.

Industrial facilities may use proximity cards or magnetic/barcoded access cards at the gate. These can be provided to employees as well as contractors. For additional security, a telephone system with remote or managed access may be installed as well.

Biometrics

Biometric access systems have evolved over the last decade and are very popular today. These types of systems include retinal scans, palm scanning, finger scanning and voice patterns. While it is virtually impossible to duplicate any of these biometrics, readers can malfunction and misidentify or not identify an authorized user.

The sophistication of these systems makes them an excellent choice for large facilities such as hospitals, nursing homes, post offices, and banks. Biometrics offer built-in fail-safes that cannot be replicated or forged. Access to certain floors in multilevel buildings can be restricted based on the predetermined rights assigned to the individual, managed by access, group, or rule.

There is also a wide variety of keypads and PIN pads available for biometrics. Biometric scanning devices that include keypads are some of the most popular applications. In the event the scan fails, the individual has the option of using the keypad to identify themselves. Having a backup such as this is beneficial to entities with a large number of employees. Since every attempt is recorded for review, the system administrator has the history and can review and correct any issues.

Near field communication (NFC) card readers

NFC is relatively new to access control systems. The basic premise of this technology enables a variety of devices (even smartphones) to establish radio communication by either touching the two devices together or placing them within a certain proximity. These devices utilize electromagnetic induction between two devices with loop antennae.

Readers can range in price from $187 for an AMG-I60C Proximity Card Reader to $2,479 for the Panasonic AJ-PCD30PJ - card reader - USB 3.0.

Lock Hardware

There's a variety of locks and locking hardware available for your access control system. Below, we discuss the most popular combinations. The first being door locks, for which there are two types: magnetic locks and electric strikes.

Magnetic locks

Magnetic locks use an electromagnetic mechanism and armature plate to create a lock that is nearly 100% reliable. When the lock makes contact with the armature plate, a current is passed through the system that secures the door, making it impossible to open. Magnetic locks also simplify remote access control, easily triggered to provide access to an individual viewed from

a security checkpoint or even through a mobile device. Their simplicity and dependability allow them to be used for everything from apartment complexes to emergency exit doors.

Depending on your security needs, it's important to be aware that there are two different kinds of magnetic locks: fail-safe and fail-secure. **Fail-safe locks** are unlocked if power is lost, making them suited to retail stores and other areas that require emergency exits. **Fail-secure locks** remain locked in the event of a power loss and are therefore used to secure areas that house valuable goods or sensitive data. Battery backup is an option but it must be checked and replaced regularly and is not intended for long-term operation.

Maglock systems start as low as $599 for a complete single door magnetic lock kit from Cobra up to $2,499 for the Cobra Controls ACP-4T 4-door Computerized Access Control System KIT. Your costs will vary depending on the level of sophistication needed for each location. Most businesses use a combination of lock hardware types to accommodate the level of security needed at each door.

Electric Strikes

An electric strike is mechanically-operated. The strike releases a door when the mechanical part is activated, such as pressing a panic bar from inside the building. During a power outage, this is possibly the best solution for door security. In fact, almost all emergency exits in establishments are equipped with electric strikes.

They can also be activated by an electronic controller outside the building and work with card readers or other types of access control devices.

If you are equipping your access controlled doors with both of these types of locks, you need to install an RTE or RTX button (request-to-exit), so that when the panic bar is pressed, you retain ultimate security. This set up is highly recommended for all types of industries.

Perimeter locks

Elevator control is available via keypad, card swipes and biometrics. Elevator and floor access can be assigned to an individual, group, or by role and managed just as easily. These assigned rights can be changed at any time, both from the control panel as well as remotely.

- **Pricing tip**: The cost for these devices can run from a $10 to upwards of $1,000, depending on the type of device and sophistication. Programmable devices land on the costlier end of the spectrum.

Assess your business needs to determine the type of device that is required at each entrance and exit point. By planning carefully, you can design the most efficient access control system with the correct type of lock hardware at each location. Because within the same facility there may exist a need to vary the levels of security and locking systems.

For example, within a hospital or doctor's office, accounting records need one type of security level while regulated drugs require a much higher level. The same holds true for financial institutions.

Fences, rolling gates and swing gates will more than likely require magnetic locks with electric strikes. Access control can be managed, granted by way of cards, keypads, proximity devices, or keys.

Features

As you shop for and design the best layout for your access control system, you'll notice a growing number of companies offering products that are more robust. The newest now include add-on features as part of the standard package.

We cover the most popular features below.

- **Timing**: refers to setting specific times when doors should lock and unlock. This provides extra security with the ability to lock down a section of the facility while others are functioning.

- **Tracking**: Access control software can provide excellent metrics that will let you know who has entered the facility, at what time, how long they stayed and what time they left. The software can also track employee access to any area of the facility that is controlled and report any attempts to access restricted areas. In addition, it can provide information on who was on-shift during any special occurrence or event.

- **Audit trail**: This feature ensures you have total access to all historical data and that it is backed up properly. If possible, request a "test drive" of the system.

- **Mobile security**: This allows total remote control of the system. Be sure to discuss the Remote Access Control Tree to ensure you have assigned proper levels of authority for remote access.

- **Backup options**: Consider remote or cloud backup to your system. In the event of drive failures or catastrophes, this will enable you to investigate the events of the day and rule out such things as arson or sabotage

The more sophisticated the system, the more expensive it will be. Consider the value of your combined assets, including personnel. What kind of price tag would you put on your employees' security? Selecting the best combination of features and designing the right

system to protect ALL your assets requires some time and cost comparisons – a process that can be greatly simplified with the assistance of a professional access control dealer.

Choosing a Dealer

Now that you have an understanding of the different types and components that make up an access control system, it's time to choose the best one. A critical piece of that decision will be the dealer you work with. Below is a list of suggested points to cover when speaking with a dealer to gauge if they are the right choice to work with.

Installation

Every installation will be different. Start by showing your consultant the layout of your facility to help them identify your needs as they relate to internal and external access control. In addition, define all necessary sub-categories. For example:

- Computer servers
- Financial records
- Personnel records
- Regulated substances
- Hazardous materials
- Facility access/exit points
- Equipment
- Security offices

With the design framework established, there is a basic installation process that is common to all. In short, your dealer will set up the configurations for your doors, computers and control devices, and whichever type of technology you select for identification. Expect them to integrate all of these devices into your local server, establishing administrator rights and passwords as well as all access levels. They will then troubleshoot the entire system before turning it over to you.

If you have a large facility, you may consider bringing your access control system online in increments to minimize disruptions.

Integration

After tying all of the access control components together, integration continues. If you use additional business efficiency platforms such as time and attendance software or monitored alarm systems, you can save considerable money on IT maintenance and labor costs by ensuring they integrate with the access control platform you're considering.

Be on the lookout for an access control system that offers plug-in integration. This framework enables you to quickly and seamlessly combine all of your business systems into a single platform, eliminating the costs and inefficiencies associated with multiple independent systems. It also provides a far more comprehensive search function that encompasses system-wide results.

Training

Though basic systems are going to be pretty self-explanatory, a couple options exist for training your employees on the functionality and operation of an access control system. Often taking the form of workshops and seminars, many provide hands-on experience with the products themselves and can be a helpful way to 'try before you buy'.

Some training programs are offered on-demand depending on the size of the group while others are conducted at a dealer's facility and require advance registration.

It's also worth noting that many manufacturers offer product seminars at trade shows and through authorized dealerships. This can be an easy way to find local information and demonstrations on the access control products you're interested in.

Support and maintenance

With so many parts contributing to the whole, regular service and maintenance is essential to keep your access control system up and running. In particular, high-use items like card readers and door locks need continuous maintenance to avoid failure.

When comparing dealers, give preference to those that provide high levels of support for reactive maintenance and preventative maintenance. Timely responses to issues related to reactive maintenance are essential when a component fails or the system experiences a glitch. Preventative maintenance can often minimize these glitches by ensuring all software updates are current and installed properly, and any integrated systems are compatible and in sync with the latest updates.

Most dealers now offer some form of online support, whether it's an online database for self-service during off-hours or live web chat. In addition, all dealers provide some form of telephone support, though many tend to cut it off around 5 p.m., local time.

Customizations

Access control platforms are easily customized through plug-ins. Popular options often include:

- Physical access control hardware
- Remote access
- Biometric components
- Access limitations
- Expandability
- Visitor management platforms that track visitor traffic

Keep in mind that the more inclusive the system is, the more it will cost. So if there are unnecessary bells and whistles in a system you're considering, ask about the availability of a stripped-down version to save on cost.

Codes and regulations

Ask your dealer about the codes and regulations that govern the types of locks acceptable for use on access and exit points. Generally speaking, any door that serves as an emergency exit and is equipped with panic hardware (also known as a crash bar) may not include any other type of locking device per the National Fire Protection Association's (NFPA) 101T Life Safety Code. The code goes on to state that these types of doors must open in a single motion.

In addition to the NFPA regulations, the International Building Code also stipulates a range of different codes that impact the use of electromagnetic locks with access controlled egress doors. Most notable among them is that any loss of power automatically unlocks the door.

Cost breakdown

By some estimates, post-sale support and maintenance account for nearly 70% of the total cost of an access control system. This makes it one of the more pertinent considerations when comparing dealers.

Expect to pay anywhere from $10 to $100 per month on average depending on the size of the system and the inclusiveness of the service. Other estimates range from $3 to $5 per ID card (essentially charging for the number of users in a system).

It's worth noting that the average cost among major brands is currently between $51 and $60 per month and includes a basic access control hardware package (mainly designed for small businesses). Large operations with customized platforms should expect to pay on the higher end of the range and above.

Choosing a dealer

Though the above criteria offers a pretty clear picture of whether or not the dealer you're considering will pair with your business needs, there are two final options that can provide additional insight into the way a dealer does business:

- **Background and experience** – Give preference to dealers that can provide examples of systems they've installed within your industry. This familiarity with your line of business has been shown to improve the return on your investment by incorporating tools and customizations you may not think of or even know were available.

- **Reviews/references** – Check with the Better Business Bureau and conduct a thorough web search for online reviews. While this should never be the sole basis for a purchase decision, these resources offer tips on the level of quality provided and how well the company deals with problems. Also ask for a list of references then use the names provided to get details on the strengths and weaknesses of the products and support services.

###

About Purchasing.com

In business since 1992, Purchasing.com has connected nearly 5 million buyers with pre-screened, qualified sellers. Our current seller network exceeds 3,500 top brands and continues to grow every year. With a history built around helping procurement officers and SMB owners make smart buying decisions, Purchasing.com has positioned itself as an essential resource and first stop in the B2B purchasing process. Our mission is simple: help buyers save time and money by providing robust purchasing guides and buying resources and matching their buying needs with pre-qualified suppliers offering customized price quotes.

Visit http://www.purchasing.com to learn more.

Contact us

888-977-4788
info@purchasing.com
Twitter: @Purchasing_com
Facebook: http://www.facebook.com/purchasingdotcom

Partner with us

If you are interested in partnering with Purchasing.com and you're a qualified supplier of industrial equipment or services, contact us at sales@purchasing.com.