Umbrella TECHNOLOGIES

PLANNING FOR A SUCCESSFUL ACCESS CONTROL SYSTEM INSTALLATION

THIS COMPLETE GUIDE WILL HELP YOU IN THE PRELIMINARY RESEARCH AND AREAS TO ORGANIZE WHEN YOU ARE PLANNING FOR AN ACCESS CONTROL SYSTEM INSTALLATION

Planning for an electronic door access control system installation is no easy task. Depending on how large your facility is, how many employees, how many doors both entrances and exits (plus interior) there are several directions you can go down before you get into what specific access control manufacturer or product to choose. This guide will help you to organize and plan for the operational challenges and technical difficulties.

Umbrella
TECHNOLOGIES

Here are the 5 basic steps you need to follow for Access control system installation:

IN THIS GUIDE

You will have a detailed information of installing an access control system.

01

Planning and Designing

Plan ahead to meet future expectations.

02

Procurement

Look for a reliable security partner.

03

Project Management

Work towards the plan.

04

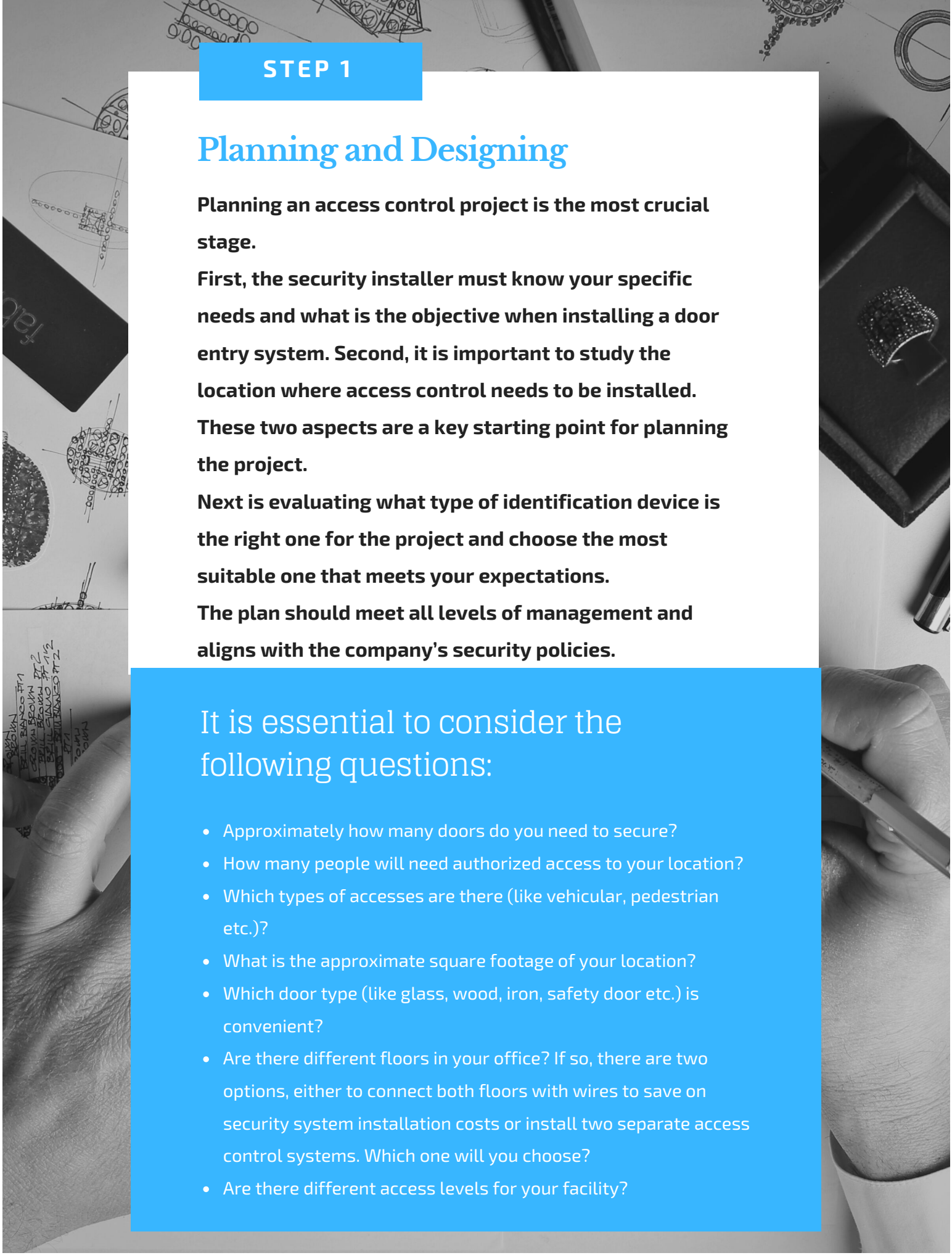
Testing and Maintaining

Test in all possible ways.

05

Training

Train your clients.



STEP 1

Planning and Designing

Planning an access control project is the most crucial stage.

First, the security installer must know your specific needs and what is the objective when installing a door entry system. Second, it is important to study the location where access control needs to be installed. These two aspects are a key starting point for planning the project.

Next is evaluating what type of identification device is the right one for the project and choose the most suitable one that meets your expectations.

The plan should meet all levels of management and aligns with the company's security policies.

It is essential to consider the following questions:

- Approximately how many doors do you need to secure?
- How many people will need authorized access to your location?
- Which types of accesses are there (like vehicular, pedestrian etc.)?
- What is the approximate square footage of your location?
- Which door type (like glass, wood, iron, safety door etc.) is convenient?
- Are there different floors in your office? If so, there are two options, either to connect both floors with wires to save on security system installation costs or install two separate access control systems. Which one will you choose?
- Are there different access levels for your facility?

Design Stage

The design stage includes identifying **different access types** that will fit the plan, locate different readers and controllers to be aware of the real distance between them, different types of equipment, access point hardware's that can withstand the temperature, the capacity of the power supply shall be selected to meet the largest load and the right cabling to connect the hardware devices.

Once everything is in place, a Facility Security Floor Plan is created outlining cable paths for installation, identifying secure doors & outlines specific hardware to be used at each secure door location.

An expert on door access control installation has the specialized knowledge to be able to determine the correct access control solution or assist you with these decisions.

Umbrella
TECHNOLOGIES

STEP 2

Procurement

Several copies of the Facility Security Floor Plan are made and send to few reliable security partners to benchmark the prices.

It is hard to find a good and reliable security partner. There are security system companies like Umbrella Technologies, who can not only help you in installing your door security system but also guide you throughout the process of planning and making the right decision.

Once you decide on the security partner, an agreement will be signed for the implementation of the door access system which should include a long-term preventative service agreement.

Umbrella
TECHNOLOGIES

STEP 3

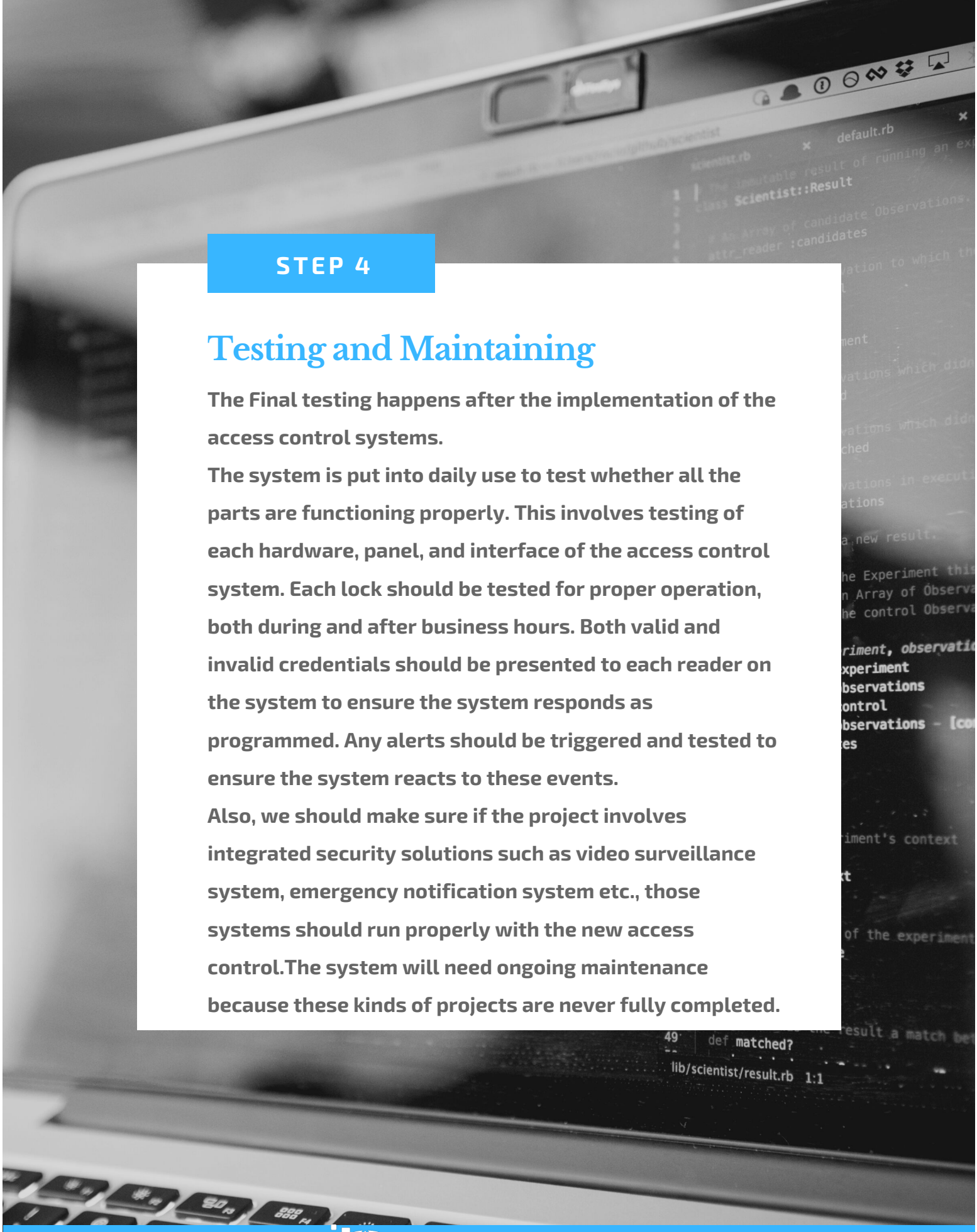
Project Management

A project schedule is made that depends on the scope of the project.

The employees should be notified by the organization about the planned work on-site by technicians. The security partner should communicate with the organization's point of contact about each day's progress.

All software and hardware should be installed and tested prior to replacing any old devices with new ones.

Umbrella
TECHNOLOGIES



STEP 4

Testing and Maintaining

The Final testing happens after the implementation of the access control systems.

The system is put into daily use to test whether all the parts are functioning properly. This involves testing of each hardware, panel, and interface of the access control system. Each lock should be tested for proper operation, both during and after business hours. Both valid and invalid credentials should be presented to each reader on the system to ensure the system responds as programmed. Any alerts should be triggered and tested to ensure the system reacts to these events.

Also, we should make sure if the project involves integrated security solutions such as video surveillance system, emergency notification system etc., those systems should run properly with the new access control.The system will need ongoing maintenance because these kinds of projects are never fully completed.

Umbrella
TECHNOLOGIES

STEP 5

Training

Finally, you will be trained by the security partner on how to operate the system and various operational challenges.

Each stage of installing access control involves specific knowledge of some sort. Experts in this area, such as Umbrella Technologies, can provide a seamless access control installation. Contact us today for expert advice on door access control system installation.

Umbrella
TECHNOLOGIES

WHO TO GET INVOLVED?

It's important that the individuals in charge at your facility include other perspectives from department heads when planning your access control installation.







From our experience here are the roles and value they can bring in the planning phase:

FACILITY MANAGERS

Facility Managers understand the building. They would be the go-to person for construction, cable-paths and potentially areas of risk.
A Facility Manager is like a security manager, who operates at different levels within your organization. They are responsible for making sure that the facilities and their services meets the need of the employees who work in them. Their common duties include inspect facilities and properties proactively, address safety concerns, responsible for property maintenance, institute security electronic door locks like key fobs, security door codes etc., be aware of the emergency notification system floor plan and guide employees during such events. In short, Facility managers have the knowledge and understanding of each nuts and bolts of your facility, thereby becoming an important personnel in the access control installation process.

HUMAN RESOURCES

Human Resources plays a vital role in employee identification, securing employee data and access management. They control the database of employee information such as job title, department etc. These information's are critical for providing access rights based on various factors such as role, responsibility, department etc., which can be readily available from HR team. They even manage who should have access to what. Thus, HR team can help you in figuring out which teams or employees should have access to which doors in your facility.

Umbrella
TECHNOLOGIES

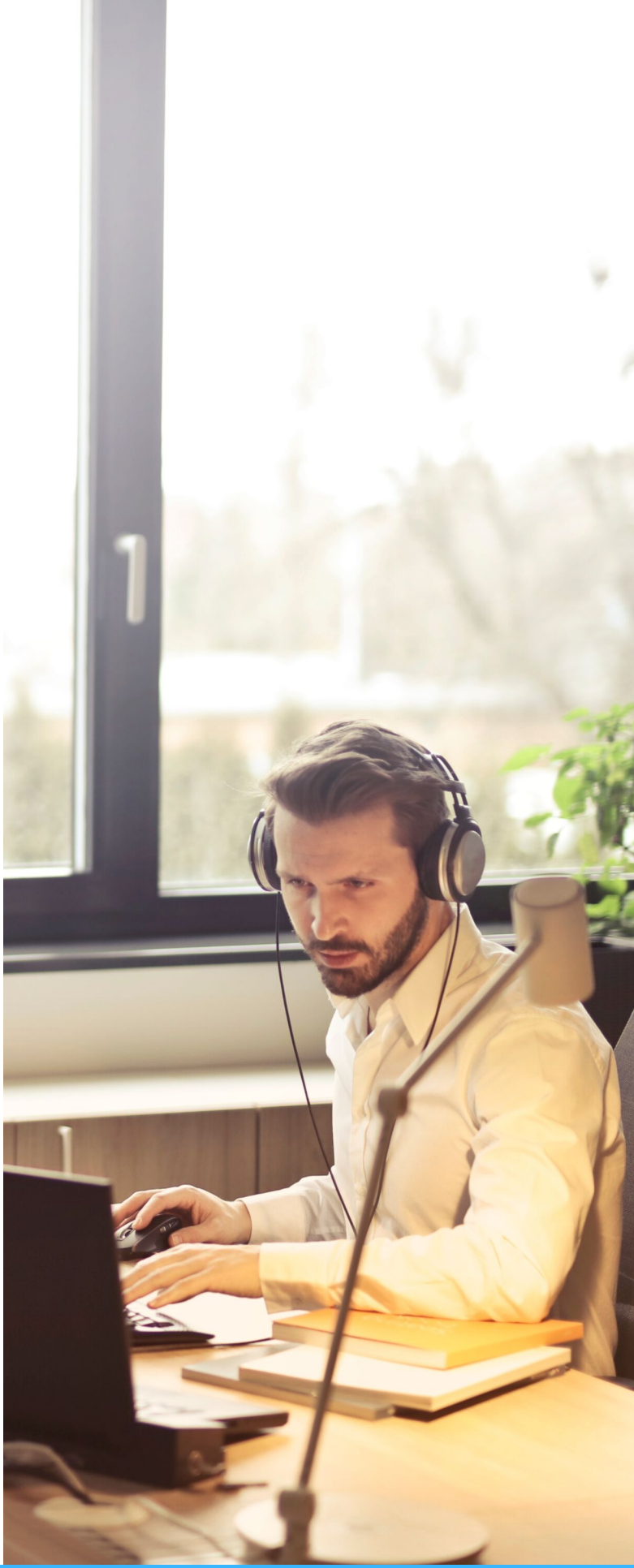
SECURITY MANAGERS

Security Manager's duties are similar to a Facility Manager. They assess risks, establish policies to protect the employees, staffs and other individuals in your organization, Identify integration issues, spearhead mitigation procedures, forensic investigations and vulnerability audits. It is important to be aware of the security policies and measures of your organization before planning to work on access control installations.

Umbrella
TECHNOLOGIES

DIRECTOR OF IT

Considering access control systems are now large in part of the internet of things- they will be going on your network and will probably be hosted in the cloud depending on if you **choose a cloud or on-premise access control system**. The IT administrator will be a vital asset in vetting the technology and ensuring it will run in parallel with your established network on inclusive of your IT department.



Umbrella
TECHNOLOGIES

OPERATIONS & ACCESS LEVELS

Auditing your organization to determine who has what level of authorization is critical. Different job functions have different responsibilities all of whom should have different access levels within your company. We highly recommend from the start you create Access Groups which is a profile established for a specific role which will ultimately determine their access level.

As part of this due diligence you want to establish what areas of the facility this role will have access to and when. Take into consideration the shift when the employee is on, if they would need access outside of their normal shift and what areas of your facility are critical to their productivity.

Establishing access groups will make your system repeatable for on-boarding new employees in the future.

Users with the Manage Access Levels permission can assign individuals to a different access level after they are accepted. An organization individual can only be assigned to one access level. Each organization has two standard access levels: Administrator and User. You can create, modify, and delete the access levels. When you create a child organization, it has the same access levels as its parent organization. But it's important to note if a child organization already exists, and you create a new access level in the parent organization, the new access level is not created in the child organization.

A map of your facility can help you in planning out what areas needs which type of access. It can be partitioned with different color schemes based on the access levels. You can start with the main entrance of the facility that allows employers to enter or exit the facility. From there breaking it down to different blocks or towers of the facility to different floors and deciding on which areas different employees needs access to.

The most important fact of this whole conversation is each employee should have the right access based on their roles and responsibilities. Access levels are determined by Facility manager or Employee supervisor.

In most of the organizations, an employee is given a user role or a role-based access or a team location-based access to the area of your facility. When an employee requests a particular access to that area, an approval request is sent to the supervisor or the facility manager, who grants the access to the employee if it's an authorized access. The approval request is generally a form with employees' basic information where the supervisor or facility manager needs to fill the time and days the employee is in the building and sign off the request. It's better for you to automate the process by connect the access control systems with HR employee information database so that when an employee leaves the company or terminated, the access is revoked automatically.

DIFFERENT ACCESS LEVELS BASED ON ROLE FOR YOUR FACILITY

Owners

They have complete administrative access to your facility. This role should be limited to a few people in your facility. They have full account access, including service configuration, account management capabilities and user access control.

Users or Members

The default role for everyone else in your facility. This type of access allows a person to view statistical data, analytics, build, deployments and service configuration information for all services on an account.

Financial or Billing managers

Allows a person to manage billing settings, view billing information about an account. View statistical and analytical data for all services on an account.

Billing managers can:

- Upgrade or downgrade the employer's account
- Add, update, or delete payment methods
- View payment history
- Download payment receipts
- View, invite, and remove the billing managers

Engineer

View configuration and setup details, build and deployments, make configuration changes, including activating new services, troubleshooting various issues using log files etc.

TYPES OF ACCESS PERMISSIONS IN YOUR FACILITY

EDIT OR READ AND WRITE

This permission level allows users to view the information and add, edit, update or delete it. The teams with the Edit permission level can:

- Access projects
- Add child organizations or branches
- Change configurations or settings
- Manually trigger builds and deployments

READ

This permission level allows users to view different projects or reports and download them. The teams with the Read permission level can:

- Access projects
- View outcomes
- Build reports and dashboards
- Perform various analytical models
- Download documents

ADMIN

This permission level is rare and only given to few individuals in an organization based on its role. The teams with the Admin permission level can:

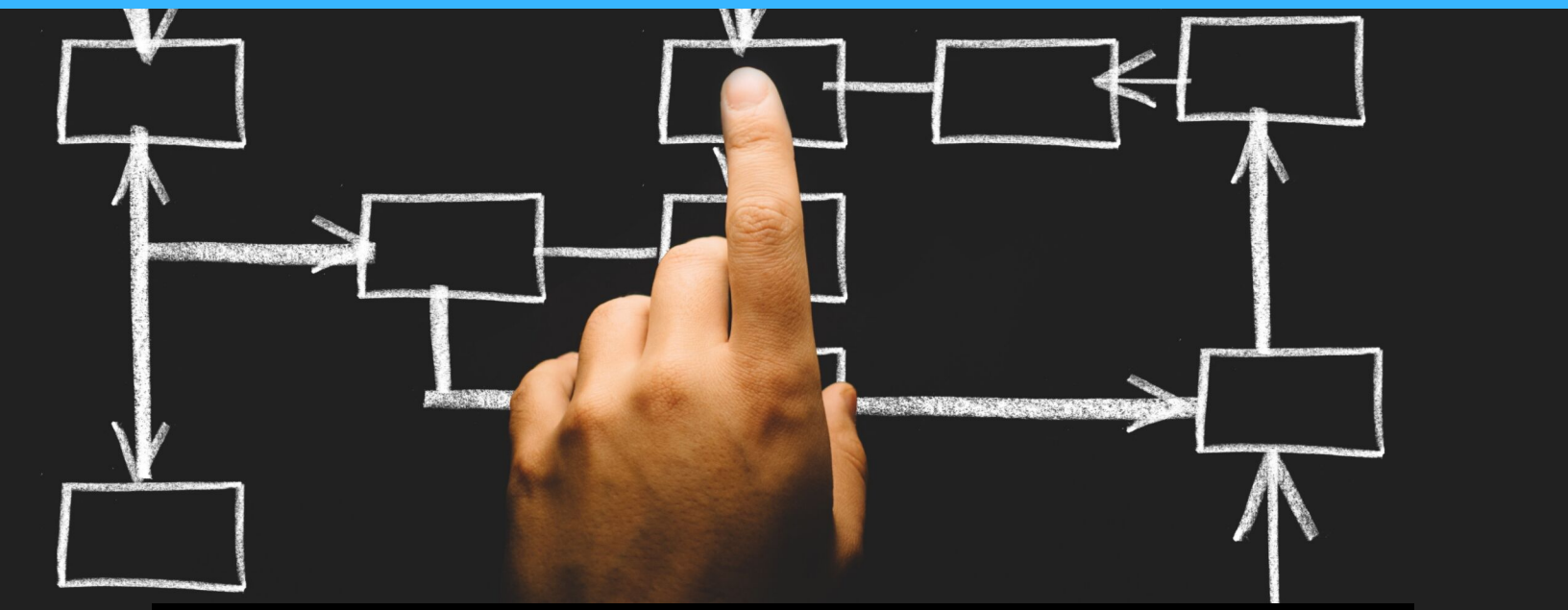
- Access projects
- Change configurations or settings
- Add child organizations or branches
- Manually trigger builds and deployments
- Add and remove projects from the organization account
- Manage confidential information

OWNER

This permission level has full control of the facility. The Owners team is able to:

- Access projects
- Change configurations or settings
- Add child organizations or branches
- Manually trigger builds and deployments
- Add and remove projects from the facility account
- Manage teams
- Manage billing information
- Edit the facility profile
- Delete the facility account
- Manage confidential information

SETTING UP ACCESS LEVELS FOR YOUR FACILITY



Access levels allows you to set wide range of permissions for your users accessing a facility. Access levels are presented as numbers (You can use any numbers), where application assumes that user with lower access level has lower permissions and can access only a limited set of information. On the other side, the user with highest access level have highest permissions and can access the most sensitive and confidential information on the system. The system administrator sets up a hierarchy of users based on their roles, duties, departments and other factors. The users between lower access level and highest access level have access permissions accordingly to the hierarchical structure. This procedure of granting access permissions is known as access rights.

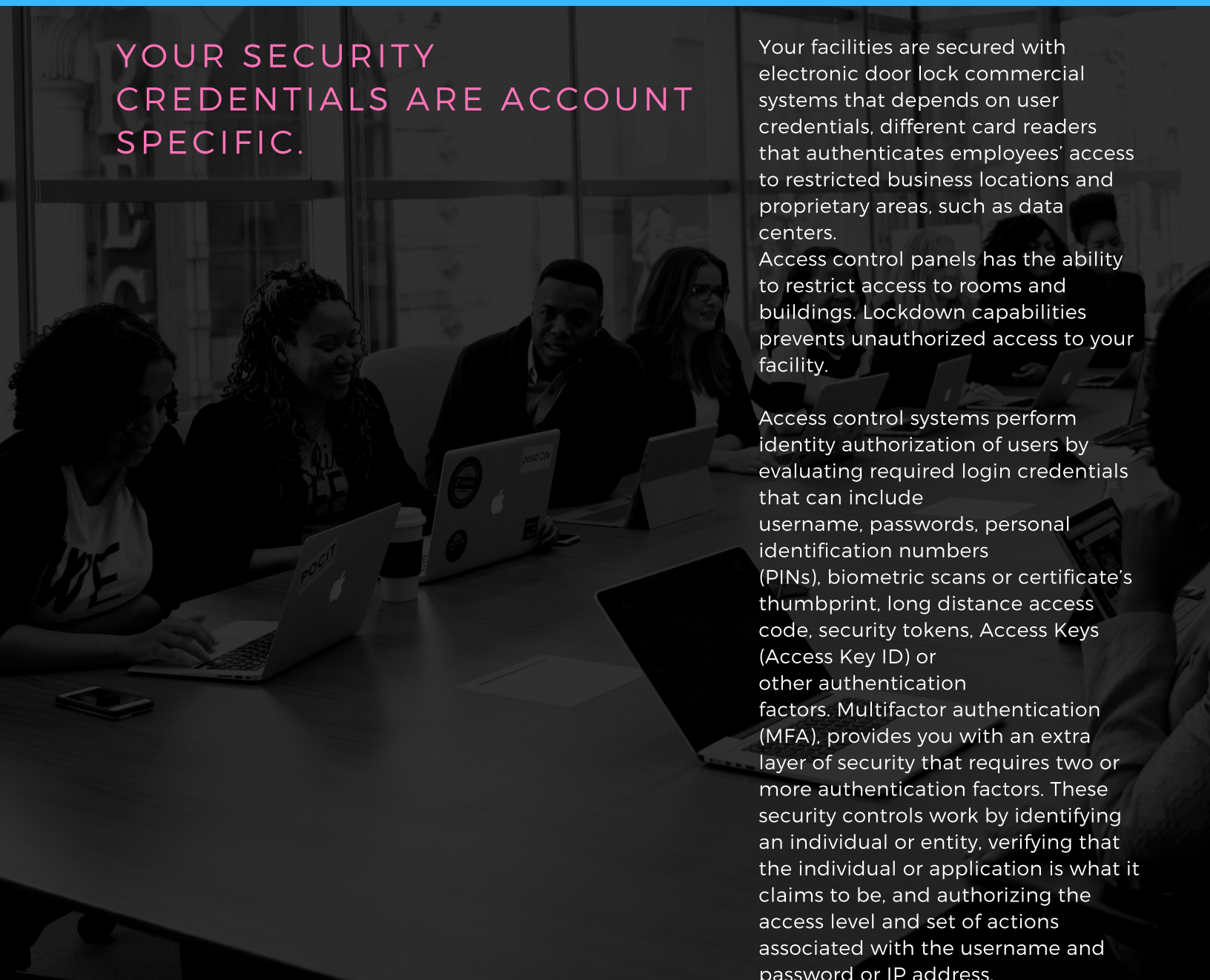
Let's consider an example,

Access levels are determined based on the organization's requirement. You may grant limited lower access level to visitors, who has access to only few areas of your facility like lobby or cafeteria and grant higher access level to employees, who are placed above the visitors in the hierarchical structure.

You may also determine based on user's roles and responsibilities like cashier as limited user, managers as users performing some critical business operations and an admin with unrestricted or full access. You need to prioritize the access levels and you can achieve that by setting the access levels in the system application like the below levels in the example:

0	Default for limited users. Will be able to access unprotected or non-confidential application sections only.
2	Employees who can access the necessary areas of the facility depending on the type of work or based on department.
4	Senior Employees who can have more access permissions than the new onboards or employees at lower level in the hierarchy.
5	Can be assigned to Managers and allow them to view reports in management sections, perform various audits but no permission is granted to edit or delete documents.
9	This level can be assigned to "master admin", who will have unrestricted or protected access to all sections, sensitive data and perform any actions.

SETTING UP SECURITY CREDENTIALS FOR YOUR FACILITY



YOUR SECURITY CREDENTIALS ARE ACCOUNT SPECIFIC.

Your facilities are secured with electronic door lock commercial systems that depends on user credentials, different card readers that authenticates employees' access to restricted business locations and proprietary areas, such as data centers.
Access control panels has the ability to restrict access to rooms and buildings. Lockdown capabilities prevents unauthorized access to your facility.

Access control systems perform identity authorization of users by evaluating required login credentials that can include username, passwords, personal identification numbers (PINs), biometric scans or certificate's thumbprint, long distance access code, security tokens, Access Keys (Access Key ID) or other authentication factors. Multifactor authentication (MFA), provides you with an extra layer of security that requires two or more authentication factors. These security controls work by identifying an individual or entity, verifying that the individual or application is what it claims to be, and authorizing the access level and set of actions associated with the username and password or IP address.

Features and Capabilities of your Access Control System

Access control systems plays a vital role of ensuring the security of your business. These **systems controls individuals' access to different entrances or exits of your facility** and establish access levels for areas of your office. It authenticates the identity of the individual and cross references against the employee information database to attain the access authorization level.

They record employees or visitors access history in the facility to maintain security of your organization. Advanced technologies are used to identify the individuals seeking access to your facility or a restricted area and allows access only to the areas aligned with their permissions.

THERE ARE SEVERAL PHYSICAL TYPES OF AUTHENTICATION

Key fob
A small security token that uses RFID technology to control your access to buildings, computer systems, network services and data. Generally carried on a keychain.

Micro Tag
A sticker that uses HID proximity technology. Converts a photo ID to a proximity card by tagging into a nonmetallic device. It easily attaches to a mobile device and other objects.

Electronic access card
A physical card that can be swiped or scanned for entry.

Biometrics
Fingerprints or facial recognition that identify the individual seeking access.

Password or pin code
Users can enter the correct password or pin code into a keypad to gain access.

Mobile apps with barcode
Users download the app to their phones and generate a barcode that they scan in the barcode reader to enter your facility.

The authentications require a reader to gain access. Card Readers are generally mounted on the exterior (non-secured) side of your door that they control. There are several types of readers:

Keypad

The access control keypad has numeric keys arranged in a block or pad with digits, symbols or alphabetical letters just like your calculator or push-button-telephones. A keypad allows only a single-entry code. These locks can either be mechanical with no battery usage or electronic in some cases with some type of power source.
The single-entry code is used to authenticate the user and requires entering a correct numeric code to gain access to your facility. When access control keypads are used in addition to your card readers, both a valid card and the correct numeric code must present before access is granted.

Biometric

Biometric replaces the use of password, pin codes or key fob; Your Finger becomes the key to your business. These systems use biometric devices such as fingerprint or thumbprint readers, facial recognition scanners, retinal eye scanners and hand geometry readers.
Biometric access control is either used for authentication or identification of the users in your facility. When your smart card is brought in close proximity to the biometric reader, it authenticates the identification of the cardholder by comparing the finger presented to the reader with the template stored on the credential. Your Card with biometrics eliminates the possibility of a stolen credential. A standalone biometric reader is used for identification of the user. The finger is matched with database of enrolled templates.

Proximity Card Reader

A contactless smart card that functions by holding your card in close proximity to the reader. It uses the RFID technology. The Proximity Card Reader is wired to your access control panel. The wires carry power to the reader, and data transmits from the reader to the panel. The Reader emits an electromagnetic field. Card access system works when your proximity card is brought within the field, the card absorbs some of the energy from the field. The card converts this field energy to electrical energy, which allows the electronic circuits in the card to "turn on" and transmit its number to the reader. The reader sends the card number to your access control panel, which looks up in its database to see if the card number is valid and if it has rights to open that door at this time. If the card access is granted, then the control panel sends a signal to the door lock to unlock for a certain period of time.
The card data transmission distance varies with your card type and reader type. The distance at which your card will successfully transmit data to the reader is called the Read Range. The read range is approximate and can vary depending on the details of your installation. Maximum range is achieved when the reader is mounted far away from metal and cards are presented parallel to the reader face. This allows the card reader field to power up the card transponder at a farther distance.

ONCE YOU'VE HAD ALL THE INPUT FROM DEPARTMENT HEADS, ORGANIZED YOUR GROUP AND SECURITY STRUCTURE, NOW WOULD BE A GOOD TIME TO CREATE A CHECKLIST OF FUNCTIONALITY YOU WANT FROM YOUR ACCESS CONTROL SYSTEM INSTALLATION. THERE ARE THINGS TO AVOID SO MAKE SURE TO ALSO READ

"The Biggest mistakes when upgrading your facilities Door Access Control System"

The access control system you choose needs to be a functional part of your business. It's something your organization will rely on daily and choosing the right solution is critical. From our experience here is a check list of functionality or features your access control system should have.

01

AUTHORIZED ENTRY

This feature allows you to keep track of the individuals who gets in and out of your facility. There are various technologies that works inside the system to grant or deny access if it's an unauthorized access. Integration with emergency notification systems will allow you to receive instant alerts if an unauthorized person attempts to access your facility.

02

ONBOARDING

Automate processes with existing employees simplifies the Onboarding process. For example, new joiners get access to the same courses or programs, in a cloud-based format, on their own time.

03

CUSTOM ACCESS LEVELS

You can create several access levels for your employees and staffs in a hierarchical order and give them permissions accordingly as we discussed above.

04

FLEXIBILITY

You will want to use a system with flexible hardware and software. With a flexible system, you can make changes to cardholder records, add, edit and delete information fields as needed.

05

EASE OF USE

You would always prefer to use devices that are less complicated.

06

SCHEDULED BACKUPS

With whatever access software package you choose, you will want the ability to schedule backups of the access control database.

07

AUTOMATIC LOCK AND UNLOCK DOORS

You can set up a schedule for certain doors to lock and unlock automatically. This is done for buildings that are open to public or unprotected areas.

08

CUSTOM REPORTS

A true access control system records each time the card is accessed at your facility and stores it in the database. So, when you need to determine who was the last person to access a particular door, you would have the ability to run a report that would show you.

09

LOCKDOWN MODE

Some of the access control system has this unique feature. It disables all users from accessing one, a few, or all entrances of your facility. This is mainly designed to restrict employee access until a manager arrives on the scene. The door will not open until a valid master card is used to access the facility, or until the lock down mode is lifted.

10

CUSTOM ALARM NOTIFICATION

You can set alarm notifications to make different sounds, which makes it easier for you to differentiate between emergency and non-emergency situations.

11

INTEGRATION

Access control systems can be well integrated with other systems like emergency notification and video surveillance systems so that everything can be managed from one user interface.

12

CLOUD MANAGEMENT

It allows you to access data from anywhere and at any time.

13

SCALABLE

Access control systems are expandable. It has the ability to manage commercial security systems from one to hundreds of facilities and grow your business.

14

ROBUST SECURITY

More than just door security; these systems can provide a complete security solution.

15

REMOTE MANAGEMENT

Allows you to remotely control lock or unlock Doors, Revoke Access and manage your website or view reports on desktop, tablet or phone.

16

MOBILE MANAGEMENT

You don't forget your mobile! An effective access control allows individual to access your facility with mobile devices. This is a smart approach for a modern organization.

17

EMAIL OR TEXT NOTIFICATIONS

You can set up your system to email or text you during emergency situation such as if a reader is down or if a door is left open.

18

INDIVIDUAL ACCESS CODES

Employees in your facility have unique identity. The doors at your facility will only allow them access if it's a valid access that matches the person's identity.

19

REAL-TIME ACCESS TRACKING

You can track the status of every door who accessed your facility in a single glance. Some systems not only allow you to see whether a door is locked, unlocked, propped or forced but it also allows you to change the state from your mobile devices.

20

RELIABILITY

A reliable and flexible platform that adapts to new or existing IT infrastructure.

- Supports the following:
- Multi readers and controllers
- Unlimited site, device and door capacity
- Unlimited credentials and administrators.

21

TECHNOLOGY

Technology that provides the highest level of security and convenience in access control today. Support for a wide range of credential technologies.

22

MULTIPLE FORM FACTOR OPTIONS

Access is granted to your facility using different physical access control devices such as smart cards, fobs, tags and mobile devices.

23

SECURITY AND COMPLIANCE

Ensure compliance through customized security reports delivered automatically via email on your predetermined schedule. Provides High Security, High-performance, maintenance-free.

24

AUTOMATIC UPDATES

Always keeps your system up to date with real time software updates.

25

VISITOR MANAGEMENT

Having the ability to track visitors using the access control system can also be valuable. Some of the more sophisticated visitor management systems today can integrate with access control systems so all door transactions will be managed and recorded in one system.

26

BATTERY BACKUP

It keeps your facility secure for hours, even during a power failure. Cloud backup really helps you to secure your data during a system outage.

27

CENTRALIZED MONITORING

It enables your users to access all applications, websites and other computing systems from a single profile, with the same credentials from any location and multiple devices.

28

UNIFIED SECURITY PLATFORM

Integrated security systems for businesses such as access control, video management, identity management, visitor management and emergency notification systems provides you with a more secure and flexible system that allows businesses to effectively protect their facilities, transform their business operations and meet compliance.

29

WEB-BASED INTERFACE

It provides an extra layer of security to your business by collecting data on all events that occurs within the system. You can control the system's settings from anywhere and anytime.

30

AUTOMATED ADMINISTRATIVE SYSTEM MANAGEMENT

Your systems will be automatically updated with the latest version of software's as soon as they are available and system backup will be done on time.

31

EVENT MANAGEMENT AND REPORTING

Displays access control events and stores them for customized reports.

32

IDENTITY MANAGEMENT

Provides identity management solution for badge generation and ID photo capture.

Umbrella
TECHNOLOGIES

NOW THAT YOU KNOW THE PROCESS AND REQUIREMENTS FOR A SUCCESSFUL INSTALLATION OF AN ACCESS CONTROL SYSTEM, IT'S IMPORTANT TO BEGIN FURTHER PLANNING WITH A PROFESSIONAL SECURITY INTEGRATOR.

WE AT UMBRELLA TECHNOLOGIES WANT YOU TO HAVE THE BEST ACCESS CONTROL SYSTEM POSSIBLE THAT FITS YOUR BUSINESS NEEDS AND SPECIFICATIONS. CONTACT US TODAY.

LET'S TALK