

A White Paper on Access Control Benefits

By Mace Security International 

Why Use Access Control?

The Purpose Of This White Paper

The goal of all Mace Security Products white papers is to provide our customers and prospects a better knowledge base to make an informed decision on utilizing new security technologies.

Summary

Locks and keys allow you to secure your building, but when keys are lost or stolen, the inconvenience and expense of changing locks and re-issuing keys can be considerable. Keys may also be copied, creating even more security risks.

All businesses, whether small, medium or large, have assets that need to be protected from theft. There is also the issue of protecting staff and their property. It is common in buildings that are secured by locks and keys for doors to be left unlocked all day. This increases the opportunities for theft, malicious damage, and violent acts.

Why Use Access Control?

Electronic access control provides the most efficient and convenient way of securing your building and assets. Installing an access control system eliminates the need for changing locks. Tokens are issued to allow access through the controlled doors, and are easily barred from the system if they are lost, stolen or just not returned.

Once an access control system is installed, all doors controlled by the system will automatically lock when the door is closed. Anyone without a PIN or access token is unable to enter. If necessary, doors may be set to unlock during a designated time frame.

Access control can also offer flexible control over users' access rights. For example, all staff can gain access through the main door of a building, but access to internal areas may be restricted to those who have a specific need to be there. Access may also be restricted by time, only granting access to particular users at certain times of day or night.

The need-to-know principle

The need to know principle can be enforced with user access controls and authorization procedures and its objective is to ensure that only authorized individuals gain access to information or systems necessary to undertake their duties.

The organization must develop and maintain a set of policies and procedures covering system users:

- identification
- authentication
- authorization

Accountability and Reporting:

Systems generally have audit trails (records) and logs to associate a subject with its actions. The information recorded should be sufficient to map the subject to a controlling user. Audit trails and logs are important for:

- Detecting security violations
- Re-creating security incidents

Many systems can generate automated reports based on certain predefined criteria or thresholds, such as:

- More than three failed logon attempts in a given period
- Any attempt to use a disabled user account

These reports help a system administrator or security administrator to more easily identify possible break-in attempts.

Central control

Access Control software gives you full control over the access control system from one location. Any instructions given to the software in a properly set up system are immediately updated at all the doors. Adding users, barring users and changing users' access permissions are done from one central location.

Access permissions may be set individually or by department. Some areas may be restricted to only a certain group of users. Shift patterns may be set for departments, and those permissions are allocated instantly when a new user card is issued.

The Value of Wireless Access Control

Pulling wire is one of the most labor-intensive and costly activities of a security system installation. With the growing use of access control systems in facilities, secure ways of avoiding that expense are often preferred by security dealers, systems integrators and their customers.

In addition to avoiding the time and expense of a wiring installation, wireless access control systems can be advantageous for retrofitting in existing buildings where wiring installation might be difficult, such as concrete block or historic buildings, and for connecting to remote locations, such as guard houses or gates, and other buildings.

Wireless systems are limited by signal strength and signal transmission. This may be overcome by the use of a bridging or repeating device. The number of devices available will be dependent on the system you use. Generally the Bridge/Repeater plugs into your computer network and allows wireless communications with the wireless Access Control Units.

You can have various numbers of devices on a system, each one of them controlling Access Control Units.

The Bridge/Repeater provides the wireless communication link between the PC running Access Control software and the Access Control units. If the Bridge/Repeater is Ethernet capable it may be able to use a site's LAN/WAN, allowing multiple Bridge/Repeaters to be placed around a site and used to link back to the control station via the site's LAN/WAN. This means that Access Control units can be installed at a greater distance from the PC running the Access Control Software.

Conclusions

Protects Your Assets

Access Control works as a security guard on your site. It provides a highly efficient means of granting entry, while maintaining a high level of building and property security.

Protects Your Employees

The system allows entry to only those who are authorized and keeps out unwelcome intruders.

Restricts Unauthorized Access.

The electronic access control system controls who are allowed entry to every door and gate by time of day.

Provides an Audit Trail.

The access control system provides an audit trail of who is accessing your facility and when, enabling determination of who was in a specific area at an exact time if an incident occurs.

Eliminates Key Problems.

Installing an access system eliminates all the problems associated with mechanical key and lock systems, e.g. the time and cost of re-keying when an employee is terminated, the cost of duplicate keys, lost keys, tracking who has keys.

