Why controlling your keys is the first step to better security

Do you control your keys, or do they control you?

By April Dalton-Noblitt, Allegion
October, 2012

Do you know where all of your master keys are?

If the answer is no, your office security may be compromised. That's because locks alone cannot assure the safety of your property and/or the people who use it. Locks limit access only if you have control of the keys that operate them. Therefore, key control is critical to your overall security.

Key control means:

- You know to whom you have issued every key
- You have retrieved all keys from people who no longer are authorized to have them
- No keys are missing
- No key has been duplicated without authorization

You can easily lose control of your organization's keys. While the average key system is out of control within seven years, it can take less than that for your security to be compromised by a lost, stolen or improperly duplicated key. Without careful monitoring and adherence to policies and procedures, your office can become vulnerable to loss and damage, and may not be as safe as you'd want for anyone who may visit or work there.

Consider these questions about your key control:

- Are you completely certain that you can account for every key that has been issued?
- Have you retrieved every key from ex-employees/students, contractors, cleaning services or security personnel who have left your organization?
- Can you guarantee that no keys have been lost, stolen or duplicated?
- When was the last time you re-keyed your office or building?

A negative answer to any of these questions could indicate a major security problem.

How easily key control slips away

You can quickly lose control of your key program through a variety of situations. For example, in a small business environment, offices, meeting rooms and plant facilities often need to be accessible to people at all hours of the day and night. You may issue keys to employees, maintenance teams, cleaning crews or even outside organizations that rent or use your facilities after hours. In many cases, employees who have quit, been laid off or fired fail to return their keys.

The result: too many people acquire keys. These people may give keys to other people, and in turn, those people share your keys with even more people. Eventually, you have a proliferation of keys, and no one individual knows who has each key or even how many are in circulation.

Unless you have a high-security, patented key system, keys can be easily duplicated and reduplicated at will. The result: security becomes virtually non-existent.

Consequences of lost key control

Key control does not replace standard personnel security procedures. However, a well-functioning key control program is an essential part of a security program.

Consider what may happen in your facility if you do not have control of your keys. Essentially, you are giving access to total strangers and making it easy for them to perform criminal activity without a trace.

For instance, thieves can remove hundreds of thousands of dollars' worth of equipment from a computer room in just a few minutes. In addition to the monetary loss, your company's computer programs can be paralyzed for an extended period, resulting in lost productivity and the potential for compromised personal or private data. Vandals also can quickly damage property with spray paint and hammers. The most serious consequence is personal violence that can lead to debilitating lawsuits, negative publicity, a tarnished image for your facility, loss of public confidence and a resulting loss of employees.

In the case of a lawsuit lack of key control becomes an important part of the picture. Attorneys will demand to see your key control records, expect you to account for every key that has been issued, examine your procedures to retrieve unauthorized keys, and review your record of changing locks. If you can prove you have done everything in your power to make a reasonable effort toward security and protection, including key control, you have a basis for defending the security and safety of your business.

Gaining control, and keeping it

Historically, the only way to regain control of a compromised mechanical locking system is to rekey the entire facility. This process consumes valuable time and can be expensive. Often the system is quickly compromised again when an unauthorized key has been duplicated.

Today there are many options to help alleviate the need to re-key an entire facility. Some involve sophisticated technology that eliminates the need for keys altogether, and some simply require a more structured and vigilant approach to managing your mechanical security. Here are some of your options:

Smart cards

Smart cards offer the most sophisticated security available today. These cards work by exchanging information with a credential reader in a process called mutual authentication. This dual layer of communication between the reader and the card is unique to each card and cannot be compromised. Smart cards also work harder to support a variety of functions like cashless vending in a cafeteria to network login, loyalty and incentive programs, data storage and transfer, and storing biometric templates for identity authentication.

Other credentials
Credentials range from magnetic swipe cards to proximity cards and even PINs. These types of credentials can be used alone or together to ensure a higher level of access control because it's easy to remove the access rights for these credentials from the system – rendering them useless. PINs can work in combination with cards to create an even greater level of access control. Credentials also offer a cost savings in the long run because there is no need to re-key locks and issue new keys if a card is lost, stolen or damaged.

Patented keys
These solutions offer the most reliable option when using mechanical keys. If a patented key is duplicated, the manufacturer will take legal action for patent infringement, not against the key holder, but against the locksmith or the company that made the key. This is a strong deterrent against unauthorized duplication.

Restricted key blanks
A restricted key blank is not available to everyone. The manufacturer of the lock or cylinder typically requires a letter of authorization to sell the blank key. However, this restriction is routinely bypassed by aftermarket key blank manufacturers who duplicate and manufacture "generic" keys with no restrictions. Locksmiths can then duplicate the keys.

Engraved warnings
Keys may have the warning "Do Not Duplicate" stamped on them. While laws prohibit the duplication of these keys, the laws are extremely difficult to enforce. Locksmiths and retail stores routinely duplicate these keys with no questions asked.

The bottom line
The safety and security of your clients, students, patients, employees, visitors and contract or service people may be at risk if you have not addressed the issue of key control. Regain control and keep control of your facility by Identifying key control solutions that fit your office or building's needs.

Learn more about key control

For more information about controlling your keys and credentials, please contact a professional security consultant in your area by calling **888.758.9823** or fill out the **Contact Us** form on our website at allegion.com.