

The ins and outs of mechanical keys

Keys - do you control them or do they control you?

By April Dalton-Noblitt, Allegion
December, 2012

You may have superior quality locks in your facility, but locks alone cannot assure the safety of your property and/or the people who use it. In fact, locks limit access only if you have control of the keys that operate them. Therefore, key control is critical.

Key control means:

- You know to whom you have issued every key
- All keys have been retrieved from persons who no longer are authorized to have them
- No keys are missing
- No key has been duplicated

You can easily lose control of your organization's keys. Without appropriate control, your facility is vulnerable to loss, damage, and personal injury to anyone who may enter.

Key control is essential to the protection of the access to your facility. 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?
- If they have, have you re-keyed your facility?
- Do you conduct annual "Physical Key Audits"?

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

How easily key control can slip away

Key control can be quickly lost in any number of situations. For example, in an academic setting, school buildings often need to be accessible to many people after normal hours. Students and faculty are given keys to practice rooms, meeting rooms, gyms, swimming pools and laboratories. Coaches give keys to the team manager and staff. Often gymnasiums and other facilities are rented or loaned to outside organizations, which require keys for access afterhours.

The result is too many people acquire keys. These people have lists of other people to whom they give keys, and they have their own lists of others. Soon you have a proliferation of keys, and no one individual has knowledge of them all.

Often, keys can be easily duplicated and reduplicated at random. The result: security becomes non-existent.

Consequence of lost key control

Key control does not replace standard security procedures of personnel. It is, however, an essential support measure to a security program. Your need for key control becomes more clear if you consider what may happen in your facility if you do not have it. Without key control you are, essentially, 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 institution's computer programs can be paralyzed for an extended period.

Vandals can quickly do extensive damage in a destructive rampage with spray paint and hammers.

Unquestionably, the most serious consequences are rape and murder, tragedies that occur all too frequently. No facility is immune. In addition to the human tragedy, assaults can result in debilitating lawsuits that are difficult to defend against. Other consequences include unwanted publicity, a tarnished image for your facility, loss of public confidence and a resulting loss of enrollment.

All too often, prosecuting attorneys attempt to paint a picture of negligence, claiming that the building administration disregarded the safety of the public. 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 procedure to retrieve unauthorized keys, and review your record of changing locks.

If the facility administration can prove it has done everything in its power to make a reasonable effort toward security and protection, including key control, it has a basis for defense. If not, a case may be extremely difficult to defend.

Gaining control, and keeping it

The first step toward assuring that your facility is safe is to seriously examine your facility's key control and identify where potential problems.

Key control is an issue that can be easily and dangerously pushed aside in order to concentrate on other, more immediate considerations. Unfortunately, the lack of key control can lead to serious consequences when you may least expect it. And until you regain control of your facility, the threat will continue to exist and increase.

Historically, the only way to regain control of a compromised mechanical locking system is to rekey the entire facility. This is both expensive and time consuming. After a facility has undergone re-keying, oftentimes the system is again compromised as soon as the first unauthorized key has been duplicated.

To address this dilemma, manufacturers have developed many options to help alleviate the necessity of re-keying an entire facility.

Engraved warnings

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

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.

Patented keys

These solutions offer a more reliable option for enforcement than the restricted key. 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.

Electronic stand-alone systems

Advanced security control technologies use small computer chips to lock and unlock doors. Such stand-alone systems provide the added benefit of audit trails and time functions at a fraction of the cost of hardwired systems.

Hardwired access control systems

These types of systems provide an excellent solution to the problem of key control. However, costs may be prohibitive. Costs for such systems can range from \$2,000 to \$5,000 or more per door, once you have factored all the necessary expenses.

The bottom line

The security and safety of students, staff, faculty and visitors of your facility are 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 facilities' needs.

Learn more about key systems

For more information about combating security risks with key systems, please visit us.allegion.com/products/keysystems. To reach a professional security consultant in your area, please contact us at **888.758.9823** or fill out the **Contact Us** form on our website at allegion.com.

About Allegion

Allegion (NYSE: ALLE) creates peace of mind by pioneering safety and security. As a \$2 billion provider of security solutions for homes and businesses, Allegion employs more than 8,000 people and sells products in more than 120 countries across the world. Allegion comprises more than 25 global brands, including strategic brands CISA®, Interflex®, LCN®, Schlage® and Von Duprin®.

For more, visit allegion.com/us

aptiQ ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

