Are You Falling for These 3 Key Control Myths?

By Carl Hanly, CAS, KeyTrak

To attract residents, multifamily communities are offering amenities like movie theaters, dog spas, and rooftop decks. But there is one important feature properties don't typically advertise: ***key control.***

You probably wouldn't argue that key control is important, but if you've fallen for any of the following myths, you could be putting your residents at risk.

Myth #1:

We don't have to worry about key control because we use smart locks.

It might seem like smart locks have made metal keys a thing of the past, but that's not the case. In a recent KeyTrak survey on multifamily smart locks, 75% of respondents who use electronic locks also use traditional keys for storage areas, offices, apartment backups, and more. If your property has any traditional keys, you need a way to manage them.

Now, what if you have eliminated all metal keys from your property? You don't need key control, right? Not so fast. If your smart locks use physical access tokens such as fobs or cards, it's important to secure them the way you would traditional keys to prevent unauthorized use.

Myth #2:

We have a key control policy, so our community is protected.

While your apartment community likely has a key control policy, that alone isn't enough. Ask yourself:

- **Are employees familiar with the policy?**

  If employees haven't read the policy or are rusty on the details, they can't follow it.

- **If a resident claims someone misused the key to their home, can you prove you took reasonable measures to control access to keys?**

  In addition to having a key control policy, it's important to have a verifiable log of key activity.

- **How do you know who has each key, when they took it, and why?**

  An accurate key control log requires checks and balances.

- **How long would it take for you to realize keys hadn't been returned?**

  It's imperative that you immediately identify and locate any keys that haven't been returned on time, whether by checking the key log, doing a visual inspection of keys, or receiving a text alert via an electronic key control system.

If your policy doesn't address any of these areas or if you're not able to enforce certain aspects of it, it's time to reconsider your key management methods.

Myth #3:

Our keys are secure because we keep them inside a locked room on a pegboard or in a lockbox.

Keeping keys in a locked room is a good first step. However, while pegboards and lockboxes are common methods for storing keys, they're not secure. Anyone who gains access to the area where the pegboard or lockbox is contained could easily remove keys.

In addition, using pegboards or lockboxes requires employees to remember to update a key log every time they remove or return a key, meaning the record is only as reliable as the people updating it.

Instead, consider storing keys in an electronic, tamper-proof drawer, cabinet, or wall-mounted panel that automatically restricts access to authorized users and records all transaction details. Note that electronic key control systems vary in the steps required to create a record of key use. For example, some might require users to scan a barcode, while others record the details as soon as the key is removed from the system. The fewer manual steps required, the better.

Sound key control practices are a critical part of an apartment security strategy. Instead of putting your residents at risk, put their minds at ease.