Be Smart About Access Control

By Carl Hanly, CAS®, KeyTrak, Inc.

Apartment renters are smart – and I'm not just talking about their IQs. In a Schlage study, as much as 86 percent of residents of various ages said they would pay more for an apartment with smart technology, such as thermostats, lighting, or locks.

The fact that most residents prioritize locks is consistent with a different report by reputation.com, which analyzed over 400,000 apartment reviews in the U.S. and found that safety was a top factor in a positive resident experience.

It makes sense, then, that some properties are opting for keyless entry. But for some people, smart locks don't represent safety. Just ask the group of New York tenants who recently sued their landlords for the right to use physical keys instead of the building's new smart lock system, which required residents to use a smartphone app to enter the building. The plaintiffs were concerned that the system would track location data, violating their privacy.

Whether your apartment community uses electronic locks or traditional metal keys, an effective method of managing your keys and locks is non-negotiable. Follow the guidelines below to get on the right track.

Look for inefficient key and access control processes.

Do your on-site personnel have a lot of extra time? Not likely. That's why it's important to make sure they're able to balance performing administrative duties and addressing residents' needs.

Processes are important, but consider how much time employees spend on manual tasks related to unit access. That could include completing paper key control logs, reprogramming smart lock security tokens (fobs, cards, etc.), or retrieving unreturned keys.

If your processes are cumbersome, employees are more likely to omit steps and find shortcuts. For example, I worked with one community that programmed master versions of fobs so employees didn't have to program a token every time they needed access to an individual apartment.

As a result, it was easier for employees to misuse their privileges because the property's electronic logs didn't show who had been in each apartment. Employees had more time to focus on residents, but it put those same residents at risk due to a lack of accountability.

To address this risk, the property instead pre-programmed a fob for each apartment and managed the fobs with an electronic key control system. Employees saved time, and the property manager was able to track who accessed each unit and when.

No matter your access control method, make sure you balance efficiency and security.

Respect residents' privacy.

Even though multifamily residents don't usually own their homes, maintaining their trust requires you to respect their private lives and personal property. If an employee uses their access control privileges to enter a person's home without authorization or prior notice, your relationships with residents will suffer.

Imagine how someone would feel if they came home to find a maintenance technician in their home without

continued

having submitted a work order or being notified that a property employee would be entering the apartment. Or if a leasing agent used mailbox keys to steal residents' identities. Or if a maintenance technician gave a key to someone who then murdered a resident in her home. Unfortunately, these are all real scenarios described on review sites and in news reports.

To avoid similar situations, ensure employees give proper notice when they need to enter a resident's home and maintain a reliable record of who has accessed which apartments and when.

Consider your reputation.

Your reputation can take a hit from a single lost key or security breach. If a resident has a bad experience, they won't hesitate to talk about it online. I've found several security-related complaints in property reviews I've read. Here are a few examples:

- Residents mentioned maintenance technicians entering units without prior notification and lamented the property's recurring theft problem.
- Reviewers described the property and staff as "creepy" and "terrifying."
- A community's mailbox keys and apartment keys were stolen on two separate occasions. It took weeks for the property to rekey each building and install new mailboxes. In the meantime, mail had to be hand delivered.

Reviews like these aren't going to do any favors for your reputation since 94 percent of respondents in an Entrata survey said they read online reviews when searching for an apartment.

Follow key control best practices.

To ensure your key and access control procedures maximize employees' time, protect residents' privacy, and safeguard your property's reputation, implement the following best practices:

- Observe a written policy for managing keys or security tokens.
- Regularly review your key control policy with employees.
- Don't store keys somewhere they can be easily removed, such as on a pegboard or in a lockbox. Secure keys in an electronic key control system consisting of steel drawers or a tamper-proof panel.
- Avoid programming master versions of security tokens.
- If you pre-program a security token for each unit, treat the tokens with the same level of security you would traditional keys – store them in a secure location and restrict who can access them.
- Automatically track when someone removes or returns keys or security tokens.
- Allow employees to remove keys only during specific time periods, such as during business hours or on-call days.
- Never leave keys out in the open or anywhere they could be stolen.
- Give residents prior notice when employees need to access their homes, especially if a resident hasn't submitted a work order.
- Monitor and address complaints about security concerns.

Be smart about your key and access control processes – no matter what kind of keys you use (or don't use).