

QUIZ: ARE YOUR ACCESS CONTROL METHODS OUT OF CONTROL?

By Carl Hanley, CMS, Regional Manager for KeyTrak

Secure access control methods are critical to providing your residents a safe place to live. How secure are your keys and/or smart locks? Take the quiz below to find out.

1. Do you have and follow a written key control policy?
 - A. Yes, and we stick to it.
 - B. Yes, but our employees don't always follow it.
 - C. No, because we use electronic locks.
 - D. No, we don't have an official key control policy.
2. Can you tell which employees have accessed which keys and when?
 - A. Yes, we use an electronic key control system (a wall-mounted panel or drawer-based system that digitally tracks when keys are added or removed).
 - B. Yes, they complete a written log when they remove a key.
 - C. No, but we use smart locks that show when units have been accessed.
 - D. No or not always.
3. If a key isn't returned when it's supposed to be, do you know about it?
 - A. Yes, we limit how long keys can be checked out and know immediately if they haven't been returned.
 - B. Yes, but it sometimes takes a while to review which keys are still checked out.
 - C. No, we use a smart lock system and can revoke unit access electronically.
 - D. No, we don't always know when a key isn't returned.
4. Do you give vendors keys?
 - A. No, an employee is required to give vendors access to units.
 - B. Yes, but only if the unit is unoccupied.
 - C. No, but we grant temporary access via our electronic locks.
 - D. Yes, we give vendors keys to use for maintenance purposes.
5. Do you use master keys?
 - A. No, we don't keep master keys.
 - B. Yes, but we reserve their use for emergencies only and there are limits on who can remove them.
 - C. No, but we use a smart lock system that allows us to program access to multiple units through security tokens such as fobs or cards.
 - D. Yes, we use master keys when showing units, performing maintenance, etc.
6. Could an unauthorized person gain access to keys?
 - A. It's not likely. Our keys are stored in a locked room inside an electronic key control system.
 - B. Only if they were able to break into the room where we keep our keys.
 - C. No, we use electronic locks.
 - D. Possibly, if they figured out where we store keys.

7. Do all employees have access to all keys?
 - A. No, we restrict access to keys by role and by shift times.
 - B. We don't have official rules, but our access log shows who's accessed which keys.
 - C. No, we use smart locks that require employees to have access privileges to program locks or security tokens.
 - D. Yes, all employees can access all keys.

To evaluate your responses, use the following answer key.

ANSWER KEY

Mostly A's: The Key Control Pro. Keep up the good work! You keep your keys secure by storing them in a safe location, such as inside an electronic key control system within a locked room. You restrict employees' access to keys (unit keys only — no masters!) and have an up-to-date digital record of who accesses which keys and when. If someone doesn't return a key when they're supposed to, you follow up with them immediately.

Mostly B's: The Middle-of-the-Roader. You realize key security is important and have some key control policies and processes in place. You're heading in the right direction, but some of your key management practices could be putting you at risk, such as not enforcing the key control policy, using honor-based manual logs to keep track of keys, or keeping keys in a place that's not as secure as it could be, such as a room that's not locked at all times or a cabinet that can be forced open. Re-evaluate your policies and educate yourself on best practices.

Mostly C's: The Smart Community. You've implemented electronic locks, but make sure you're smart about how you manage them. While keyless entry systems seem to eliminate the need for key control, many still have a slot for traditional keys as a backup option or use security tokens such as fobs or cards that function like keys. Have a plan for how you'll manage these backup keys and security tokens. Also restrict who is authorized to program security tokens and avoid programming master versions of cards or fobs.

Mostly D's: The At-Risk Property. Your property doesn't have firm key control policies and uses risky practices such as using master keys for daily tasks or keeping keys where an unauthorized person could remove them. Get control of your keys ASAP to keep your residents safe and protect your property from liability.

Carl Hanley is a regional manager with KeyTrak, Inc., where he has worked for 20 years. He specializes in helping multifamily housing, student housing, military housing and corporate housing clients conveniently minimize risks associated with managing their resident keys. He has received his Certified Apartment Supplier (CAS) accreditation from the National Apartment Association (NAA) and has completed NAA's Leadership Lyceum training. He is actively involved with the NAA National Supplier Council.