Essential Key Control Strategies for Housing Organizations

In today's housing environment, effective key management is critical for maintaining security, ensuring operational efficiency, and protecting the assets of housing organizations. With an increasing need to balance safety and accessibility, housing organizations must implement comprehensive key control programs to manage access, reduce liability risks, and enhance overall operational effectiveness.

This guide highlights the core elements of a well-structured key management program, from tracking inventory and defining access protocols to documenting policies for staff, tenants, and vendors.

An effective key control program provides many benefits to your housing organization, including but not limited to:

- **Improved Security:** Unauthorized access to buildings poses many risks, including potential criminal activity and building damage. Failure to execute adequate key control may also result in reputational damage for your agency. Strong security practices at your organization can help defend against potential and costly liability claims.

- **Operational Efficiencies and Cost Savings:** Documented procedures and up-to-date inventory lists will allow your organization to conveniently determine if/when to replace key hardware. You won't spend money unnecessarily on hardware that may not need to be changed. In turn, this may allow the organization to invest in other security measures with those cost savings.

Core Components of an Effective Key Management Program

1. Managing Key Access and Tracking Inventory

Maintain an inventory of all keys, identify the key types, and document who can access master keys. Management should also document which employees have master keys or keys to more sensitive areas of buildings.

Key types and systems:

- **Standard Keys:** Also known as common or unrestricted keys, standard keys are easily duplicated and do not require special permission to make additional copies.

- **Restricted Key System:** This system helps control standard key duplication. A restricted key system prevents unauthorized duplication of keys. The system uses patented key blanks. Duplication can only be requested by and granted to registered users on file. Restricted keys cannot be duplicated at local hardware stores. This rule allows for better security and can result in cost savings over time—your organization won't have to re-key locks every time an employee leaves, as long as they return the restricted key. You can feel confident knowing that no additional copies are lying around.

- **Electronic Key System:** This system requires an access card, key fob, fingerprint, facial recognition, or some other credential to access a building or part of a building. This type of system allows your organization to restrict access based on time, date, area of building, individual, etc. It can also provide an audit trail. For example, you can identify who accessed the building and at what time. It also allows your organization to remove access immediately upon receiving notification of a lost or stolen credential (i.e., key fob), termination of an employee, or eviction of a tenant.

2. Documented Protocols for Changing Key Hardware

Develop written guidelines to follow in situations where locks need to be changed. Depending on the type of lock/key equipment, this may be a task your organization completes regularly. For example, vacated units that use standard keys need their locks replaced.

- Written guidelines should include:

  > Situations that require locks to be changed

  > Expected turnaround times

  > The process to have the locks changed

  > Contact information for responsible parties, such as internal maintenance staff or external vendors/locksmiths

  > Documentation requirements detailing how and where information will be maintained when locks are changed

  > Average, or expected, costs associated with changing a lock

Note: If your organization utilizes an electronic key system, procedures should reflect the same overall objectives.

- Understand the risks of not changing over locks when warranted. Although it may become costly for your agency, there could be significantly higher costs should a security incident arise from failing to secure your facility. Always respond to and document tenant requests to have their locks changed over.

3. Policies and Procedures

Develop written policies to address key controls for staff, tenants, and vendors.

- **Tenant policies** should outline their responsibilities for key control, including financial penalties for failing to return keys upon lease termination, rules prohibiting duplication of keys under any circumstance without prior approval from management, and instruction to never give out copies of keys to any individual not listed on the lease. Should your organization utilize an electronic key system, these policies also apply—instruct tenants never to give out their key code.

- **Staff policies** on key control should outline role-based key issuance to ensure only authorized personnel have access to specific keys or sensitive areas of buildings. Keep in mind that access to all tenant keys should not be available to all maintenance and/or property management staff.

- Staff should sign off to acknowledge the policy upon receiving access to keys. The policy should state that they must always keep keys secure while in their possession. The policy should also outline expectations regarding whether keys are to be returned in a lockbox at the end of each day and whether they will only be using the keys to access areas of the facility that are for direct business needs and never in an unauthorized manner. The policy can also include penalties for failing to follow all guidelines.

- The policy may also include restrictions on duplicating keys or providing a copy to any other individual. Your organization may also require reporting any lost or stolen key to management as soon as possible and that keys be returned at the end of employment (this is why it's important to keep inventory and document what keys each employee has in their possession).

Managing Vendor Access to your Buildings

Many organizations have various vendors and contractors accessing their buildings from time to time. For example, your organization may lease rooftop space to a local cable company to install cell phone towers. That vendor will need to access your rooftop to monitor their equipment. There may be times when they need access after-hours during an emergency repair.

Develop procedures to control vendor access to your building. In most instances, providing external contractors with any master key to the building to access at their discretion is not recommended. This opens your organization to potential security concerns and can be challenging to track when they have accessed your building. You may require a staff member to grant access to the building and escort them throughout their time in your facility. On the other hand, your organization may opt to greet them upon arrival, provide them with the access keys they will need, and then have them drop the keys back off when they have finished their task.

To avoid security gaps, written procedures relating to vendor access to your building should be clear and consistently enforced.
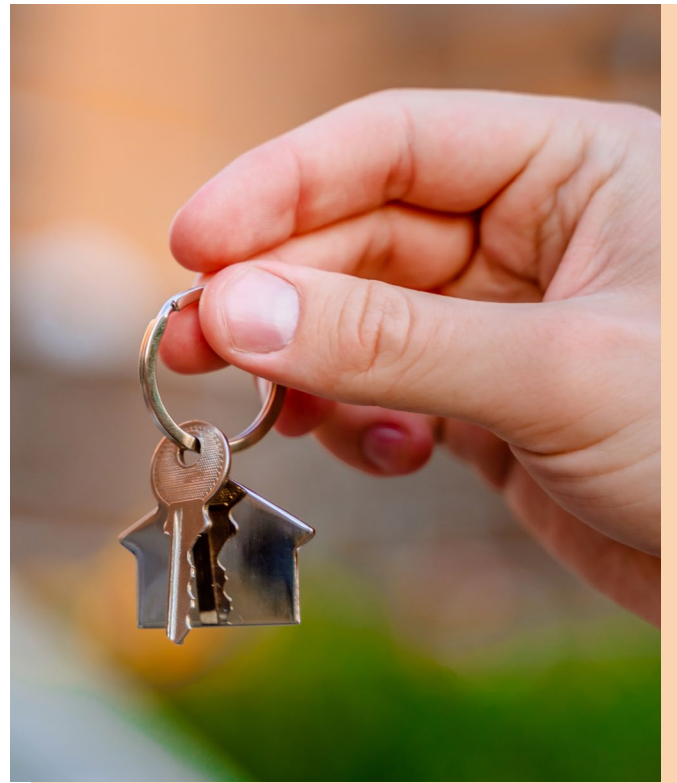
Organizations that utilize an electronic key system are at an advantage when managing visitors to the building. By using keys in the form of fobs, swipe cards, or biometrics, access can be programmed to specific individuals and restricted to only the appropriate areas relative to their services. Another benefit is that the system generates electronic audit trails each time the individual(s) accesses your building. This time-stamped and identifiable information will be available should your organization need to review records of incidents within the building.

Bottom line

A proactive, well-documented key management program is essential for securing housing facilities, protecting staff and tenants, and ensuring smooth, cost-effective operations. By implementing clear policies and robust tracking systems, housing organizations can minimize risks, improve security, and allocate resources more efficiently, creating a safer, more reliable environment for everyone involved.

Interested in working with HAI Group to manage your agency's risk?

Contact us for assistance and answers today!

Contact Now

HAI Group®

www.haigroup.com