

## Entry Code Technology – Rewards and Risks

**Keyless entry locks, and cards with chips that identify the authorized user, offer a convenient and effective system for secure accessibility. You can secure access to apartment and condominium buildings, garages, community-use areas and units. However, they also carry liability risks for landlords and property managers if not used properly.**

Let's start by looking at the good these systems provide. First, they offer real convenience. Systems can be coded so that one code or one pass card opens front gates, building doors, and community-use rooms. They can also be set up to permit intercom connections to residents so visitors can be "buzzed" in to parking lots and lobbies. These cards are more difficult to duplicate than keys, so their use can minimize the number of people with access; moreover, reprogramming cards or keypads regularly is much less expensive than re-keying locks.

Keyless systems can also be used to allow contractors and delivery people access to an otherwise secured building or complex. That can cut down on the need for gate guards, though having some human monitoring - either face-to-face at the point of entry or via a remote camera - is very important for real security.

Some keyless entry systems also provide an audit control feature, which allows the condo association or apartment manager to track who has entered the facility and at what time. They can also be programmed to unlock doors only during certain hours, which keeps people out of pools, gyms, etc. during non-operational times.

While keyless entry technology offers convenience and an affordable alternative to key-and-lock systems, it has to be done right to prevent security lapses. Keypad codes need to be changed regularly and frequently to minimize access by former residents and others with whom a code might have been shared. Changing the code also forces vendors and contractors to update their employee-access rosters. Some companies provide individual codes for each resident that can be deleted when that person moves to minimize former resident access. Cards or key fobs can be highly customized and can be deactivated when someone moves or if they lose their card or fob.

If you are using entry codes for your front gate, parking garage or building doors, make sure residents understand that allowing others to enter without putting a pass code in or using their card can lead to security breaches and possibly crime in your complex. Encourage reporting of any car that follows through an open gate without using the pass code or card. Establish rules for buzzing in visitors, and make sure posted intercom directories don't reveal full names and unit numbers.

Keeping systems in top working order is important as well because residents will quickly tire of intercoms that garble or distort voices and key pads or cards that don't work the first time, every time. It's a very short distance from that inconvenience to user by-pass of the system.

Since these systems are electronically controlled, a battery backup is necessary in case the power goes out. During times of power loss, an open building is an invitation to criminals. No matter what system you choose, always be sure to keep track of who has access to your buildings and units. Your insurer needs to know about all security systems you put in place, and you need to be sure security vendors you work with have the right commercial insurance in place, as well. Talk to your insurance agent about your liability for building and unit security and about quality risk management programs that can reduce your chances of problems.

Posted by [Global Administrator](#) on 1/28/2014 3:31:22 PM