ZURICH®

Key Control Management

Please route to:

- Owner
- General manager
- Sales manager
- Service manager
- Office manager

Vehicle theft is a thriving business. Cars stolen from new car lots, thefts from service lanes, cars missing from used car lots, and carjackings present a consistent threat to car dealerships. Thieves will go to any length to steal cars, trucks, sport utility vehicles, minivans, and motorcycles. How do you protect your inventory and customer vehicles?

Good key control is an essential element of any theft prevention program. Let's review three basic principles of key control management.

Number one: Separate the keys from the vehicle

Vehicle keys and key FOBs should never be left in the ignition or anywhere else inside or on the vehicle. This is an open invitation for someone to steal the vehicle. Keeping the keys and the vehicle separate is critical.

This sounds like basic common sense, and it is. But how often do employees leave keys in a vehicle just for a moment when they need to run into the building or take a phone call. Employees should be trained to never exit a vehicle without the keys in hand. This rule should apply to all vehicles whether it's a parts truck, customer car out on a road test, or part of the inventory.

Keys should never remain inside a vehicle overnight, not even within a secure area, such as a showroom or service department. Cars have been stolen many times while stored inside a service area. New cars have also been stolen right from the showroom floor because the keys were left in the ignition or on the dashboard. (Consider the liability if a child were to start a vehicle and take a short test drive around the room). Thieves break into the building, find a car with the keys in it, and then drive it out the door. Removing the keys from the vehicles and locking them inside a safe, office, or even in the technician's toolbox may be enough to deter a thief.

Number two: Secure all vehicles

Whenever vehicle keys are not actually in use, they should be secured in some fashion. Ideally, they should be locked in a safe or locking steel cabinet, but inside a locked office and out of public view will generally suffice. You can also consider instituting other security measures as well. Keys may be locked inside a building, but how secure is the building? Burglar alarm systems will help to ensure the keys are really protected against theft.

Keys in service areas are also vulnerable. Many businesses leave customer keys hanging on an open keyboard where anyone (vendors, delivery people, customers, contract service personnel, etc) could walk by and take them. Assigning someone responsibility as a 'work dispatcher' is the best way to safeguard keys. Keys should be assigned to technicians by the dispatcher then returned when the work is done.

The keys can then be sent to the cashier to wait for the customer to pick them up. Using this system, the keys can be accounted for at every step in the process. Unsecured keys can end up anywhere, and the same can be said of the vehicle. There are few experiences as embarrassing and unprofessional as calling a valued customer to tell them you've lost their car.

Number three: Have a system for accounting for each and every set of keys

The issue of unsecured keys is a good introduction to the third principle. Someone in the organization must be assigned responsibility for vehicle keys. Without accountability, there can be no key control management. It is the most critical aspect of any key management program. If keys to any vehicle are missing, and you cannot pinpoint the last individual that had possession of them, your key control management system is vulnerable.

A number of different systems can be used to maintain control of your keys, and they don't have to be expensive or complicated. Restrict access to vehicle keys and assign responsibility to one person for signing them out. A key log should show who checked keys out, date, time, reason for taking the keys, and when they were returned. This log should be reviewed at the end of every day to ensure that all keys are accounted for. Automated systems are also available that require employees to input a code to receive keys and record all pertinent data. These key machines are capable of producing a key report that can be reviewed to reconcile keys.

Conclusion

Theft prevention is the goal of the key control management program. It is important to keep close watch over customer and inventory keys to eliminate the opportunity or temptation for thieves. It is also the primary line of defense against professional thieves. Don't allow your assets and reputation to disappear as a result of insufficient key management.

Not a customer?

For more information about Zurich's products and Risk Engineering services, visit www.zurichna.com/zdu or call us at 800-840-8842 ext. 7449.

Already a customer?

Contact your Zurich Account Executive or agent for information about additional Zurich's products and Risk Engineering services.

ZURICH®

Resilience Solutions