Entry Management: Maintaining Safety at your Local Sites

Code Management for Government

Moving employees and vendors smoothly in and out of a facility outside of normal operating hours can pose risky and potentially costly security challenges. Consider the following illustrative incidents:

A government facility had key locks on its local office doors. Each time an employee or vendor lost a key, a locksmith had to rekey the locks and provide new keys to all employees requiring access. This resulted in significant unbudgeted, re-keying costs.

Due to a language barrier, members of a janitorial crew did not understand instructions for disarming and re-arming a local office's intrusion alarm. This hindered setting of alarms, which triggered numerous false alarms. The local police soon stopped responding to any alarms from the facility, resulting in false alarm fees.

An office manager responsible for maintaining alarm access codes was consistently adding new employees and vendors, but did not always delete obsolete codes. This resulted in 300+ inactive, yet still valid, codes built up within the facility's alarm panel. A former employee passed along his facility and vault access codes to a burglar that used them to steal valuables from the facility.

Problems like these are common within the security industry. Fortunately, today's intrusion detection systems can offer simple, cost-effective solutions for these types of situations.

/ Code Management Solutions /

Entry Management: When employees, couriers, and cleaning crews all carry keys, there are many opportunities for keys to be lost or stolen, requiring expensive replacement.

Wireless locks work with inexpensive access cards to open main entry doors. If a card is lost, it can be deleted from the alarm system with one touch on a keyboard. A new card can be created quickly on site.

Other cards in the system are not affected. Unlike keys, cards can be individually programmed to allow access only to certain areas and at defined times.

The battery-powered locks are easily installed with no wired connection to the central processor required. This type of system also compiles an audit trail of all entries and can create customized reports for the activities of any individual or of a specific entry point.

tyco Integrated Security

Entry Management: Maintaining Safety at your Local Sites

Alarm Arming Management: Vendors failing to properly arm and disarm an intrusion alarm may create a major security issue. Many municipalities have police non-response policies and/or levy expensive fines after only a few false alarms. Strengthening the alarm process foolproof can mitigate the problem.

That's exactly what a modern intrusion alarm panel can do. Each credentialed user's profile can be customized to automatically re-arm the system after a programmed amount of time. For example, the cleaning crew can be given an hour to complete its job; a courier may only get 10 minutes. Once a valid vendor has entered the facility, the alarm is disarmed yet the doors remain locked to anyone without a valid access card.

Code Management: Local site managers may typically too busy – or simply forget – to delete codes when employees leave the company. In any given location, there may be 50 listed codes, but only 7-10 active users requiring access to designated areas of the facility. This can create additional risk.

One way to avoid the risk is to take advantage of a managed service from Tyco Integrated Security. When a local site requests a code change, Tyco Integrated Security central monitoring station personnel remotely upload and download from an office's intrusion panel to delete unnecessary codes—or create them for new hires. Working with our experienced and trained professionals can mitigate a potentially serious problem of leaving your site at risk.

"Many government customers I talk with have limited understanding of their code risks and don't have a mitigation plan in place."
Don Woody – Senior Technology Manager, Tyco Integrated Security

Access, alarm and code management are all important parts of managing security risk. Government facilities, down to the local site level, need to reduce potential risks wherever and whenever possible. This requires awareness of best practices as they apply both to internal processes and available solutions. Centralized management of codes doesn't automatically solve all of the challenges. A systematic approach to managing and improving your code risk profile is needed.

/ Code Management Best Practices /

// Start with a code risk assessment or audit
// Prioritize top deficiencies and evaluate where technology upgrades can help mitigate the risks
// Develop a code management policy and communicate it
// Determine how to communicate any new processes to the affected employees and vendors
// Ensure that all authorized persons have a ***unique*** code to avoid code sharing
// Track your codes and report on changes frequently
// Expire codes that are not being utilized
// Changes codes regularly
// Utilize technology to automate what can be automated
// Consider working with an integrator to perform not only the assessment, but the remediation plan

For more information, contact your sales representative, call 1.888.721.6612 or visit www.tycois.com/government.