*A Whitepaper*

MORSE WATCHMANS

# Security Practices for Hotels

Hotels may be unique in the business world, in that they have customers that plan on spending most of their time at the premises in the relatively vulnerable position of being asleep. And in most cases, the customers are also away from their homes, and don't have direct access to their friends, families, and usual support systems. Thus, to build or maintain a reputation as a safe and secure destination, hoteliers have a special interest in security and how it can be achieved while also delivering a welcoming, comfortable environment and responsive customer service.

Because of the wide variation among hotel types and locations, a single discussion of security recommendations is unlikely to cover all relevant topics. Nonetheless, in this paper we will start with some broad security items that are intended to do just that, and then follow with a more detailed look at key and asset management as one area of particular need.

## Part 1: Hotel Security Strategies

At hotels with poor security programs – and at poorly-run organizations of all kinds – security improvements are typically made just after each unfortunate security incident. This reactive approach will never develop a positive reputation for safety and security. Perhaps even worse, the resulting security system will be a costly patchwork of specific fixes that does little or nothing to prevent future security problems. What is needed instead is a proactive security strategy.

### Recommendation 1: You need a proactive security strategy, supported at the highest management level.

With a proactive security strategy, a hotel can prioritize security investments where they will do the most good and build a framework for ongoing management and improvements. It is still possible that security incidents will occur, including both unforeseen incidents and foreseen incidents where the solution had not yet been implemented, but this approach helps ensure that the most damaging potential incidents will be prevented first.


This brings us to the next logical question: What should be included in the security strategy? The answer to this question will vary depending on the specifics of each individual hotel property, because every setting is unique. Even if two (or more) hotels are of exactly the same size and design, there are always differences in the neighborhood, climate, clientele, and proximity to other places of interest (hospitals, prisons, airports, etc.), among other factors, that affect the security risks and threats and therefore should influence the selected strategy.

*"With a proactive security strategy, a hotel can prioritize security investments where they will do the most good."*


### Recommendation 2: Start with an objective assessment of the current security risks and your current security systems.

This is a critical first step, and should not be overlooked. To be effective, the hotel security strategy must align with the actual threats to, and vulnerabilities of, the property, not to an ad hoc collection of past concerns or incidents. It is also important to note that the security risks will change over time, so the assessment should be repeated

periodically to ensure that newly emerging risks are included in the assessment, and that older risks that are no longer relevant are removed. As mentioned above, the specific risks will vary, but we can suggest some categories that should be included in every assessment, including:

- ***Security Leadership:*** Who is in charge of security, and what authority do they have to undertake security projects and implement security procedures?
- ***Threats and Vulnerabilities:*** What are the external threats to the facility, our guests, our staff, and to our valuable data? What are the internal threats from any of these to another? How vulnerable are these groups to these threats?
- ***Physical Security:*** How secure is the physical space, including exterior approaches and parking areas, as well as interior sensitive areas? What access records are kept? What is the status of the physical security systems, are they being used as intended, and are they sufficient?

*"Physical security is related to IT security – physical access can be leveraged to gain electronic access."*

- ***Information Security:*** How secure is our sensitive data and IT system? How do we know? And, note that physical security is related to IT security – physical access can be leveraged to gain electronic access.
- ***Security Training:*** What security training is given to staff? How aware is our staff to security matters, and how prepared for incident response?
- ***First Responders:*** What is the relationship with the local police, fire, and medical communities? Are they familiar with the security measures at the hotel? Have they provided input on security matters?

Based on this assessment of all the applicable factors, hotel security leadership can prioritize the risks in light of their seriousness. Then, the security strategy can be updated to address these risks and action plans can be developed that take into account the costs and the availability of critical staff and expertise to complete the projects.

**Recommendation 3: Update the security strategy based on the current risk assessment, and prioritize tasks with an understanding of the costs and required resources.**

## Part 2: Example – Hotel Key and Asset Management

One security factor of particular importance to hotels is the control of keys and small portable electronic assets. We will use the term "keys" to include both hard metal keys as well as for plastic key cards of all types. Small portable assets include tablet computers, panic button fobs, and similar electronic devices that are used in support of customer service and hotel operations.

All of these items are a central part of daily operations, but they are also central to safety and security, so they are of great interest to thieves, hackers, terrorists, and other unwanted individuals. Many hotels have taken steps, or are taking steps, to upgrade their security systems and procedures with sophisticated key control and asset management solutions such as those provided by Morse Watchmans.

*"Key control technology solutions can add to the establishment's overall safety and security structure."*

Although not usually visible to the public, key control technology solutions can add to the establishment's overall safety and security structure by providing guarded access to keys, cards, cashboxes and other valuable assets that may be kept on the premises. And when the goal of a hospitality service provider is to deliver the best possible experience for the guest, a reliable and efficient method of controlling and accessing keys is a necessary step in achieving this goal.

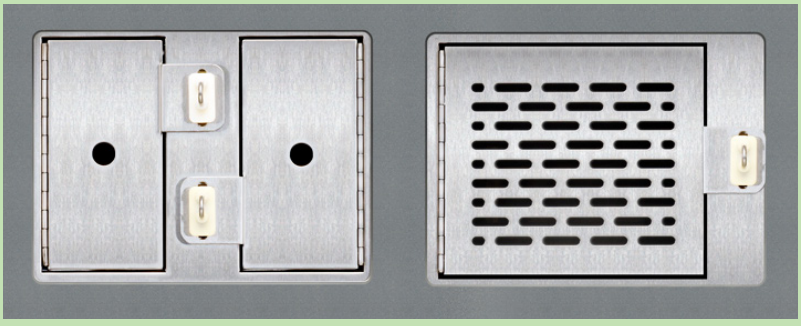
High tech key cabinets available today automatically record the access history of each key, including user, date and time of key access/return. The system releases assigned keys only to users with the proper authorization, and cannot be manipulated. The identity of users requesting keys can be confirmed in a variety of ways, including a numerical code, proximity card, fingerprint, or a combination of these. Quality systems feature rugged stainless steel construction, illuminated key slots and near indestructible key fobs, which readily accommodate both hard keys and plastic key cards, and are designed for heavy use environments such as those found in hotels. Key cabinets can often be configured with modules that hold six, eight, or 16 keys. The cabinets can also be configured with key card modules as well as large single or dual lockers to manage larger objects with the same efficiency and controls.

By integrating key control management software, facility management can more easily control the system and maximize its reporting and programmable access capabilities. Key control software can run activity reports, sort based on different criteria, and more, empowering security management and owners with highly accurate records to provide clear direction in support of controlling access and addressing security issues.

## Small Asset Management

Key management systems are a special case of managing small, important assets. With the right equipment, larger items can also be tracked, stored, and managed to be sure they are used by the right people, at the right times – all while creating an auditable usage trail to ensure compliance and generate useful operational reports.

Modular management systems from Morse Watchmans can be equipped with small lockers that operate in tandem with key management systems. These small lockers can hold company assets such as housekeeping staff panic button fobs, or personal items such as mobile phones during work shifts when they are not needed. Morse Watchmans also makes larger locker systems designed for laptop computers, tablets, radios, and similar items, with built-in RFID readers that can detect exactly what tagged devices have been stored or removed, adding an additional layer of certainty beyond just the opening of the locker door.



Small, powerful computers have been a boon to operational efficiencies and flexibility, but they have also opened up the possibility of entry points for hackers and other unintended uses. Proper tagging, tracking, and storage of these devices adds one more layer of security to these items, helping prevent unauthorized use and making it more difficult for hackers or others intending to steal guest or business data, or use as an entry point for other network intrusions.

## More Security Benefits of Key and Asset Control

Hotel key control systems provide several security and risk reduction benefits beyond other manual key management systems. Here are just three of these important benefits:

### 1. Improved Accountability

When employees know their key access activities are tracked, they have a naturally increased tendency to adhere to corporate policies and practices. For example, key management systems can be configured so that keys can only be returned by the individual who originally accessed the key, eliminating "hand offs" and the associated uncertainty. When combined with door locking systems that record who enters each door, and at what time, the resulting audit process reinforces a powerful message to every staff member – and every guest – that security matters are taken seriously and all team members are accountable for their actions.

*"The hotel should be recognized for implementing security measures which will avoid shouldering any unnecessary liability."*

### 2. Reduced Liability

Implementing meaningful controls on keys and access in itself reduces the risk of security incidents. And, having such a system in place also demonstrates that the hotel has taken appropriate actions in support of security objectives, thereby reducing the liability that might be otherwise assigned to the hotel. No one ever wants security incidents to happen, but if they do, the hotel should be recognized for implementing security measures which will avoid shouldering any unnecessary liability.

### 3. Streamlined Workflows and Reminders

Key management systems eliminate the manual procedure of signing out or returning keys, and can also be linked to time and attendance systems. When such a link is implemented, the system automatically reminds staff to return keys and other tracked assets before departing, reducing the risk that keys will fall into the wrong hands.

## Storing Panic Buttons: a Straightforward Challenge

In mid-2018, a new law went into effect in Chicago that requires hotel employers to provide a "panic button" to housekeepers and other workers who enter guest rooms. Using one of these buttons enables a worker to instantly broadcast a call for assistance from a security officer or other authority. Similar laws are already in effect in Seattle and New York, with support for legislation growing in California, Las Vegas and Miami Beach.

Panic buttons have grown in number and popularity across the country, at hotels and also at hospitals, schools and other organizations where workers are often vulnerable to harassment and other risk. The buttons typically come in the form of a key fob. For hotels and other organizations, providing their staff with panic buttons does more than comply with the law; it also demonstrates a higher level of concern and care.

Here's the challenge – how should hotel management store these fobs, and how can they demonstrate that the fobs were issued to each staff member at the start of a shift? The answer is that a key control and management system is the best way to store, track and account for panic button fobs. Each fob can be locked safely in the cabinet, and only removed or replaced by the individual who is scheduled to use it at that time. All activity can be tracked, so management gets a clear picture of employee compliance as well as an auditable record of actual usage.

## Conclusion

The best way to be prepared with a strong security system is to start with an objective assessment of threats and vulnerabilities, then match appropriate resources to a prioritized list of security improvements. The assessment should include the widest range of security topics to be sure that emerging threats are included in the analysis, not just historical threats that may no longer be the highest risks to the hotel, its staff, and customers. Cost-effective, proven solutions are available for many security issues, including key management and small asset management systems from Morse Watchmans that can be used to reduce risks, ensure compliance, and capture auditable records. Combining these solutions into an overall security strategy for the hotel, along with ongoing management and improvements, will result in the safest possible setting for staff and guests, and build up a long-term reputation for security that will serve the hotel well into the future.

**morsewatchmans.com**
(203) 264 - 4949
2 Morse Road, Oxford, CT
morse@morsewatchman.com