Hotelier Security Guidance

Implementation of Security Measures for Hotels & Resorts

Table of Contents

INTRODUCTION

This Hotelier Security Guidance provides a general guide to support and provide practical advice to hoteliers on identifying and implementing security measures at their properties appropriate to their size, geographic location and threat environment.

The aim is to provide companies with the necessary know-how which can be tailored to the specific conditions of each partner across the TUI network and is designed to complement and reinforce any existing standards, to be both practicable and reasonable, and to be as effective as possible.

The measures, however, do not substitute, prevail or alter mandatory requirements as imposed by local law or other mandatory regulations applicable. It remains your sole responsibility to comply with all of these regulations.

TUI'S HOTELIER SECURITY GUIDANCE

The guidance focuses on **having a systematic management system** in place in the hotels rather than **on the existence of specific measures**. As part of that system, special attention should be paid to the four objectives:

1. **OBJECTIVE 01 - Security Responsible Person**

    - Clearly define and allocate responsibilities for security resources, granting them the necessary authority

2. **OBJECTIVE 02 - Security management system**

    - Implementation and maintenance of a complete and thorough system – a security management system
    - Incident handling

3. **OBJECTIVE 03 - Security Risk Assessment**

    - Conduct regular risk assessments to identify and evaluate existing risks – providing resulting documentation to TUI upon request and without delay
    - Perform dynamic, ongoing risk assessment / situational awareness to continuously update the initial risk assessment.

4. **OBJECTIVE 04 - Security Awareness Training**

    - Conduct employee training
    - Develop a security culture

Knowledge hub:

This centre contains more detailed material on specific recurring topics. The Knowledge Hub will sometimes explain the frequent recurring scenarios at different depths with examples. As TUI's hotel portfolio is extensive, it is up to each hotel to decide whether the model and the solution shown can be applied to their circumstances.

Group Security third-party assessor program:

TUI is taking a risk-based approach, and with the help of its external security risk adviser company, it categorises the hotels into different risk levels. Depending on TUI's security risk rating, your unit might then be invited to one of the following types of assessments:

- Security Self-Assessment
- Remote Security Validation
- Physical Security Assessment

Our provider might also provide essential advice on potential areas for further improvement. For more information on the different types of assessments, please refer to: https://www.tuipartners.com/security/. Once the hotel security assessment is complete, an online survey will gather your feedback about the thirdparty assessor program you participated in and your experience implementing your security measures. It may be that the information on the TUI Partner's website is not meeting your requirements, and you need more assistance in deciding what actions you can take to mitigate your security risk. In that case, you may do so at your own expense by contacting a TUI's external security assessment provider or similar entity.

Security Pre-Assessment form (PSA)

The Security Pre-Assessment (PSA) form is the best way to check if your security is already in line with the TUI's Hotelier Security Guidance. Complete the PSA to understand your strengths and potential areas of improvement. The PSA form will guide you through what a sound security management system would look like in your hotel. We urge you to complete the paper as soon as possible, as it will show you any areas of improvement that you can complete before being contacted for a security risk assessment.

OBJECTIVE 01 – Security Responsible Person (SRP)

- ***Clearly define and allocate responsibilities for security resources, granting them the necessary authority***

The hotel's/resort's security management falls under the responsibility of the respective general management. It should be committed to security tasks and **provide adequate resources in the form of budget, equipment, and personnel, with the authority to make security-related decisions**.

A security responsible person (SRP) should be designated to manage directly or indirectly security tasks. The SRP should be responsible for **ensuring the deployment of the security management system and should regularly report to the hotel/resort management on the system's effectiveness and efficiency, immediately flagging any concerns to the hotel's/resort's management.** SRP is typically represented by a manager. Sometimes, especially in smaller hotels, their main role within the hotel may be something other than security.

The responsibilities of a Security Responsible Person include, but are not limited to, the following:

- Conducting & reviewing the security management system
- Ensure there is a security training program
- Report regularly on the system's effectiveness and efficiency, as well as flag any concerns to the hotel's senior management

Security requires 24/7 monitoring, which usually implies shift schedules. **These should be recorded (planned and actual) and, if applicable, also include rosters for detection/watchdogs according to the length of their deployability so that the relevant person/people can be identified in the event of an incident or investigation.**

Where it is applicable (when a risk assessment identifies the need for security personnel), the **visibility of security personnel can provide reassurance to the guests and make their stay even more enjoyable.** However, appropriate and neat dressing is essential, creating a positive perception of the security personnel. Security staff must also be friendly and approachable in case of guest enquiry. Moreover, the security personnel should be equipped adequately to perform their duties correctly while **complying with the local law.**

OBJECTIVE 02 - Security Management System

- ***Implementation and maintenance of a complete and thorough system – a security management system***

A security management system comprises all security measures, protocols, and procedures as part of your Hotel Security. TUI's external security assessment provider will focus on your management system's documentation and effectiveness. The hotel's security management system should be integrated into the overall management of the respective hotel/resort. This means a strong focus is placed on integrated measures and continuous quality management. Technical/structural, organisational, and personnel provisions should always be considered jointly because they strongly influence each other.

Quality management should be a vital component of every hotel's/resort's security management system. All security measures should be clearly planned, implemented, reviewed and adjusted/improved if necessary.

Using external partners such as security assessor companies and conducting regular self-assessments can ensure quality management is realised.

If the hotel or resort decides to outsource specific tasks which affect security management, the hotel or resort must retain control over these processes. This requires an explicit agreement to be in place, covering the definition, implementation, and documentation of measures for quality assurance over the outsourced tasks.

The security management system should be documented and reviewed regularly, with updates made where necessary. This documentation should include:

- Security policy is a general statement from the hotel/resort regarding why and how security is being managed
- Risk assessment and risk treatment methodology
- Definition of security roles and responsibilities

- Risk treatment plan
- Inventory of relevant unit assets
- Incident management procedure
- Records of training, skills, experience and qualifications
- Any additional documents which are necessary for ensuring the effective functioning and continuous improvement of the security management system

The Security Management System can be kept in digital or printed format. The most important is that it is accessible to those who need it. Some parts of the security documentation will contain highly confidential information about the business. Hence, restricted access and distribution (internally and externally) should be clarified and guaranteed.

TUI provides a **Security Management System Template**, which outlines the main objectives of a management system and contains useful templates that efficiently help you create the correct documents. Completing the Security Management System Template and following the easy step-by-step To-Do's will prepare you for Security incidents and a Security Risk Assessment conducted by TUI's external security assessment provider.

- ***Incident handling***

  a. *Develop and maintain a key contact list and keep it updated*
  b. *Prepare communication lines and public communication systems – ensuring they are easily accessible for customers – introducing processes to alert, alarm and respond in case of an incident*
  c. *Introduce process for incident reporting and investigation*

Immediate and calm management of an incident is essential to identify the seriousness of the incident, contain the damage and restore operations swiftly. Every hotel/resort should develop and implement special incident handling procedures to successfully diagnose and resolve an incident quickly and effectively. Specific risks identified during the risk assessment process should be factored in when devising incident preparedness procedures.

There are various incident severity levels, ranging from solely suspicious behaviour to near-miss situations and emergencies. Since minor incidents can rapidly evolve into serious emergencies, every hotel/resort should set out clear escalation procedures as part of their incident response process. A functioning incident alert system is essential.

The measures below are designed to introduce and/or enhance existing incident handling processes and procedures to ensure every hotel/resort can promptly respond to and resolve an incident should the need arise.

a. Develop and maintain a key contact list and implement a contact list review protocol

Reaching the right people at the right moment is key to effectively responding to an incident. Hence, every hotel/resort should have a key contact list and contact management protocol that is documented, readily available to all staff members and regularly updated. A non-exhaustive contact list of external and internal stakeholders includes:

- Internal functions (e.g. management, security personnel, maintenance team, customer services, all staff)

- State agencies, public services, local authorities and response forces (e.g. police, ambulance/hospitals, HAZMAT* response teams, supervisory authorities)
- Neighbouring properties/facilities which might need to be alerted in case of an incident of TUI functions (e.g. TUI MM, Group Product & Purchasing)
- Suppliers, contractors, external experts (transport providers, tour operators, booking agents, insurance companies, alternative accommodation, and psychological support services) or the media.

The key contact list should be **included in the hotel's/resort's security plan**. All staff members should be made aware of emergency contacts (e.g., in case of identified suspicious behaviour). The contact list should be available in digital and paper form and stored securely. A backup in both digital and paper form is required.

The security personnel responsible for communicating with external parties should be **formally assigned and authorised** by the hotel/resort's management. Designated personnel should engage with external stakeholders regularly and maintain open communication channels. For example, local police/fire/emergency services should be familiar with the hotel/resort facilities to respond efficiently and effectively in an emergency.

b. *Prepare communication lines and public communication systems – ensuring they are easily accessible for customers – introducing processes to alert, alarm and respond in case of an incident*

Every hotel/resort should develop and implement an alert/alarm/response process in case of an incident. The process should be documented and readily available to all employees.

The process should be reviewed regularly and updated when necessary to address newly assessed risks. All hotel/resort employees should receive regular training, and drills should be conducted frequently.

Every staff member should be made aware of the 24/7 security focal point person to report any incident or suspicious behaviour. Hotel/resort guests should also be informed of the presence of the 24/7 security focal point person and should be asked to report any incident or suspicious activity immediately. Moreover, guests should be prompted to familiarise themselves with the hotel's/resort's special procedures about how to behave in specific incidents such as in the event of an evacuation.

This information should be readily available in all hotel/resort guest rooms and designated common areas. It should also be accessible through the hotel/resort website and mobile apps.

For immediate alerting in case of an incident, emergency phones are strongly recommended to be easily visible and accessible to all in designated common areas (e.g. lobby, pool area, bar, cash handling areas, guardhouses, highly crowded or remote locations). In addition, discrete panic buttons for staff members are also recommended.

The 24/7 focal point person should be adequately staffed with competent personnel who are able and authorised to initiate response measures and deploy escalation procedures when needed. The hotel/resort's alert system should be easily and clearly located and accessible to the 24/7 focal point person at all times.

Incident response requires communicating with different stakeholders based on the type and scale of the incident. Hence, an individual, collective, and stakeholder communication plan should be available (e.g., provision of call circuits and apps with different distribution lists/groups).

A functioning public announcement system (e.g. loudspeakers, light signals, sirens) should be in place and cover all areas so that all people on the hotel's/resort's premises can be alerted in case of an incident. Announcement scripts for specific scenarios (e.g. fire evacuation) should be prepared in advance and made available to all staff members immediately. The announcements should be clear, understandable, loud enough,

and available in the main languages spoken by staff and guests. The use of code words, which are well known to the staff and trigger particular staff behaviour, should be considered.

For alerting and alarming purposes and ongoing communication between the hotel's/resort's security functions, backup technical communication solutions should be available. This means that the hotel/resort cannot solely rely on, e.g. mobile phones or online services to communicate in case of an incident. Alternative channels (e.g. radios, personal communication chains) are needed in case the traditional communication channels fail. Power cuts should also be considered, and an appropriate backup power supply for critical devices (e.g. server room, emergency lighting) should be installed. Moreover, depending on the hotel's/resort's location, the existence and maintenance of a satellite communication device should also be considered.

c. Introduce process for incident reporting and investigation

Every hotel/resort should have formalised incident reporting and investigation procedures. This should include consistent and detailed recording of all incidents, people involved, measures taken, and, if applicable, lessons learned and the involvement of local authorities. Crimes should be reported to the local authorities immediately and at all times. Moreover, TUI should be informed of major incidents and significant security trends/developments.

When escalating a major incident or significant security trend to TUI, please contact your local TUI representatives

Appropriate procedures should be in place to ensure an incident minimally impacts the hotel/resort and swiftly restores normal operations. All staff members should be trained on these procedures, and drills should be conducted regularly. If circumstances change, these procedures need to be reviewed.

OBJECTIVE 03 - Security Risk Assessment

- ***Conduct regular risk assessments to identify and evaluate existing risks***

Many companies make their first mistake by starting to implement their risk assessment without deciding the methodology they will use. It may sound complicated at first, but imagine beginning to build a house without any clear rules on how to do it. The best thing is to lay the regulations on the whole risk assessment process in a document for your reference. You will have to define your methods in the following areas:

1. *How will you identify the risks that could cause the loss of your assets?*
2. *How will you identify the risk owners?*
3. *What will be the criteria for assessing consequences and the likelihood of the risk?*
4. *How will you calculate the risk?*
5. *What are the criteria for accepting risks?*

If you answer these questions, your risk assessment will be **consistent** and **comparable** year to year or between units if you own more hotels

- *How will you identify the risks that could cause the loss of your assets?*

One methodology for identifying risk is the assets, threats, and vulnerabilities method, although you can approach risk assessment using various methodologies. Another option is the "Process Method", in which you analyse a sequence of steps or interactions among activities and processes based on risk sources, departments, objectives, and so on. Whatever methodology you choose should be as straightforward as possible and include

these five elements. Simply copying and adopting a methodology from other hotels, particularly larger ones, leads to prolonged risk assessment and treatment rather than completing it in just a few days.

- *How will you identify the risk owners?*

For each risk, you need to find the person who is interested in solving it and who is in a high enough position to solve the problem if it arises.

- *What will be the criteria for assessing consequences and the likelihood of the risk?*

Consequences and likelihood should be assessed separately for each of your risks. You can use numbers or simple low-medium-high scales. We recommend that you describe the conditions to be met for each scale as precisely as possible, thus ensuring consistency.

- *How will you calculate the risk?*

You can achieve this by multiplying or adding the numbers. If you have used the low-medium-high scale, this could correspond to 1-2-3 on a scale. The result provides you with the relative importance of each risk and assists you in prioritising your efforts.

- *What are the criteria for accepting risks?*

Whatever numerical risk calculation method you choose will produce a scale (e.g. 1-25); once you know how to calculate risk, you will need to decide above which figure you will need some action on. E.g. you decide the acceptable risk level is 16, any risk valued above that number needs to be treated. **If you don't want to use a numeric scale, you can decide whether you need to treat a threat or not based on your own experience and insight.**

Tips:

- First, find the methodology that best fits your circumstances
- The method you choose should contain the five elements mentioned above
- Find the right people and involve them in the risk assessment process. Department Heads will know best any potential security problems.
- It is not going to be perfect at first. It is better to do a simplified, less detailed risk assessment first, which you can return to later to review, add or modify certain risks than to spend too much time on the risk assessment.

- ***Perform dynamic, ongoing risk assessment / situational awareness to update the initial risk assessment continuously.***

The difference between a formal risk assessment and a dynamic risk assessment is that they are prepared in advance, recorded, and monitored regularly. Conversely, dynamic risk assessments are 'dynamic' or ever-changing and carried out on the spot by individuals when they enter a new environment or their current environmental changes.

This requirement has two elements:

a. *First, be aware of one's surroundings and identify potential threats and dangerous situations*

b. *Second, to continuously assess potential threats and dangerous situations and take action to eliminate or reduce risk*

a. *Situational awareness*

It is essential for personal security and a fundamental building block in collective security.

It is also important to note that situational awareness — awareness of one's surroundings and identifying potential threats and dangerous situations — is more of a mindset than a hard skill. Situational awareness is crucial for recognising terrorist threats, but it also identifies criminal behaviour and other dangerous situations.

The primary element in establishing this mindset is first to recognise that threats exist.

A second important element of the proper mindset is understanding the need to take responsibility for one's own and others' security.

The discipline part of practising situational awareness also refers to the conscious effort required to pay attention to gut feelings and surrounding events even while busy and distracted.

b. *Dynamic Risk Assessment*

After identifying potential threats or dangerous situations, one should continuously assess the risk, take action to eliminate or reduce risk and monitor and review the rapidly changing circumstances of an operational incident.

What does it mean in real life? Situational awareness and dynamic risk assessment are processes that we are all likely to do unconsciously throughout the day. For example, you walk home at night and see a group of people standing in a poorly illuminated corner. You recognise the hazard; you decide to pass by them or choose another route. In a hotel environment**, this requirement should be practised on every level consciously.** It could mean, for example, that a manager reviews the newspapers daily, listens to local news channels and looks for any signs of social unrest. Another example is when an employee recognises that somebody is doing surveillance/hostile reconnaissance at the hotel, or a suspicious item is left in the lobby and takes action.

OBJECTIVE 04 - Security Awareness Training

Once relevant security measures have been identified, staff must be thoroughly trained on all security procedures to ensure accurate implementation and monitoring. This section provides guidance on achieving this, with defined roles and responsibilities.

- ***Conduct employee training***

Security training and drills should be conducted with all staff according to their tasks and documented accordingly. All staff should be briefed on their role regarding security and the actions to be taken in case of an incident to protect themselves, guests, and the hotel/resort. Real-life scenarios should be simulated and trained for through comprehensive drills. External parties such as state security forces, emergency services, and neighbouring stakeholders should be included in such exercises to improve overall cooperation.

- ***Develop a security culture***

All staff members should be encouraged to become involved in the site's security management. This means they should understand the hotel's/resort's security approach to existing risks and how these can be encountered in their respective working environments.

Version control

Version	Date	By	Revision/changes made
Draft 01	20220318	Robert Zsolt Doma	Development
Draft 02	20220414	Robert Zsolt Doma Matthias Stresow	Review and additional Information
Draft 03	20220514	Robert Zsolt Doma	Additional information
Draft 04	20220525	Robert Zsolt Doma	Changing layout
Final v.1	20220722	Robert Zsolt Doma Matthias Stresow	Review and minor amendments
Final v.1.1	20240328	Daan Bouwsema Robert Zsolt. Doma	Changing layout
Final v.1.2	20250220	Robert Zsolt. Doma	Periodic review. Minor changes to the text without any change in content