Security Personnel

Safeguarding Your Business

☐ Prepare copies of up-to-date contingency plans, ground layout, floor plans, and locations of exit points, EHA, CCTV, AED, fire hoses and means of communication (e.g. walkie-talkies), and provide these to senior management or authorities in the event of a crisis

☐ Keep these documents and information securely, yet readily accessible to authorised personnel only

General Procedures

☐ Create and maintain an incident activity log, with an employee assigned to update it as events occur

☐ Develop a procedure to control how off-site personnel may gain access to restricted areas, both during regular operations and during a crisis

Non-Security Operations

General Procedures

☐ When handling lost room keys, verify the identity of any individuals requesting new or extra keys

☐ During peacetime, create open channels of communication with hotel administration and senior management to ensure everyone is updated promptly

☐ During a crisis, help to ensure all guests are accounted for and kept aware of any developments that may occur

Hotel Administration

Safeguarding Your Business

☐ Create templates for public communications during a crisis to prevent miscommunication

☐ Work with Senior Management to develop plans to stabilise the situation in the immediate aftermath of crises

☐ Develop post-crisis marketing and publicity plans to aid in business and revenue recovery

General Procedures

☐ When employees have resigned or are terminated, review their access rights (e.g. employee passes, biometric information, keys and passcodes) to prevent them from obtaining sensitive information or entering secure areas

☐ Create procedures to handle loss of any form of security pass (including both physical keys and digital passwords)

Incident Activity Log

Day-to-Day Operations

Ultimately, the people who work in your hotel are the ones who will ensure it is safe and secure. It is important that every employee – from non-security operations to senior management – keeps a look out for suspicious activities or individuals on a daily basis. This is critical in detecting terrorist activity or signs of cyber terrorism before it escalates to a crisis.

Security Personnel

Manpower Deployment

☐ Station employees or security officers at restricted access areas and ensure they are able to identify persons and vehicles permitted to enter

  ○ If manpower constraints do not allow you to station security officers, you could encourage all employees to look out for unfamiliar persons or utilise technology substitutes, such as CCTVs, to monitor for intrusions and cover more ground

General Procedures

☐ Look out for vehicles parked for a prolonged period of time, and question vehicle owners about their presence

☐ Enforce strict access control measures by only allowing those with employee badges and passes or authorisation letters (for third parties) to enter restricted or employee-only areas

☐ Conduct regular, but unannounced patrols and inspections at vulnerable areas, or engage a vulnerability or penetration testing service