SINGAPORE STANDARD

Code of practice for hotel security

SS 545:2023
(ICS 03.080.30; 13.310)

SINGAPORE STANDARD

Code of practice for hotel security

Contents

Foreword

This Singapore Standard was prepared by the Working Group on Review of SS 545 Hotel Security set up by the Technical Committee on Hotel Services under the purview of the Services Standards Committee.

Hotels often call themselves the 'home away from home'. Hence, as part of hospitality, it is the responsibility of all hoteliers to ensure that there is no compromise when it comes to the safety and security of their guests. As terrorism and other security threats remain significant and real, safety and security are constantly high priorities of hoteliers and guests. They are key considerations when making decisions to travel; and are critical success factors for a tourist destination. Hoteliers and everyone involved in the tourism industry need to work together to enhance the confidence of the public and our visitors.

Safety and security go hand-in-hand in a hotel. They involve protecting guests and employees from potential injury or death, as well as preventing damage to, or loss of, their property. Safety issues may arise from the effects of accidents, including fire or hazardous materials; while security issues range from crime, violence, public disorder to terrorist attacks. Hotels are expected to constantly evaluate the risk factors and threats facing them; and act responsibly to reduce their vulnerability through protective and preventive measures, including effective incident management.

SS 545 was first published in 2009 as a result of the review on TR 21 which was developed in 2005. In this revision, guidance on managing cyber security threats, data loss prevention, crisis management and business continuity was included. The standard was updated to keep abreast of technology.

This standard serves as a useful reference for hotels of various sizes in deploying daily security measures and ultimately ensuring a safe environment for their guests and employees.

In preparing this standard, reference was made to the following publications:

1. NIST Cybersecurity Framework
2. SS ISO 22301:2020 Security and resilience – Business continuity management systems – Requirements
3. TR 106:2022 Tiered cybersecurity standards for enterprises
4. WA 1:2021 Cybersecurity self-evaluation checklist and guidelines for digitalisation in manufacturing

Attention is drawn to the possibility that some of the elements of this Singapore Standard may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all such patent rights.

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as "mature standards". Mature standards will not be subject to further review unless there are requests to review such standards.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Code of practice for hotel security

1 Scope

This Singapore Standard specifies the key requirements and recommendations for hotel security to protect the physical and digital assets within the hotel premises. This includes the following key elements:

–   Security management plan;

–   Security equipment;

–   Record of security incidents;

–   Cyber security;

–   Manpower;

–   Training;

–   Areas for assessment.

2 Normative references

There are no normative references in this standard.

3 Terms and definitions

For the purpose of this Singapore Standard, the following terms and definitions apply.

3.1 Controlled access

Entry point(s) into the hotel premises for authorised personnel only.

3.2 Crisis

Situation that significantly affects the safety of hotel guests and employees, operation of the hotel or reputation of the hotel where day-to-day response plans are not sufficient.

3.3 Crisis management team (CMT)

A group of individuals functionally responsible for leading the coordinated activities of the hotel during a crisis.

3.4 Emergency

Situation that requires immediate action to mitigate or avert it from escalating into a crisis (e.g. when a terrorist threat is received).

3.5 Head of security

Person who is responsible for the security of the hotel.