Information Security Policy of the INTERCONTINENTAL® FRANKFURT

(Danube Hotels Betriebsgesellschaft mbH)

To protect sensitive information within the Danube Hotels Betriebsgesellschaft mbH (**INTERCONTINENTAL® FRANKFURT**) and protecting guest , visitor and employee data , as well as to ensure the constant availability of all relevant information and the entire Information Technology the General Manager from the **INTERCONTINENTAL® FRANKFURT** wrote the following information security policy.

Information security is a prerequisite for the business processes of the **INTERCONTINENTAL® FRANKFURT**. Information security serves no end in itself. Their goals are based on a risk-based assessment of hazards. Based on the derived appropriate measures, the availability of systems, data and services should be guaranteed, their confidentiality protected and their integrity assured. The interests of the users sufficiently into account when implementing information security.

This information security policy represents a parent document, the concrete takes place in the IT security concept and the derived Standard Operating Procedures (SOPs).

Together with the IT security concept and the Standard Operating Procedures this information security policy forms the information security program of the **INTERCONTINENTAL® FRANKFURT**.

1 Scope

This information security policy applies to all areas of the **INTERCONTINENTAL® FRANKFURT** and their employees.

As far as external service providers under fulfillment of their tasks have access to data of the **INTERCONTINENTAL® FRANKFURT** the specifications expressed in this information security policy apply to these as well.

2 Responsibility and organizational structure

Responsible for the implementation of information security is the **General Manager**. He may delegate tasks / duties within the delegation to employees in his area of responsibility.

In the field of IT security the General Manager has appointed an **IT Security Officer**. The **IT Security Officer** is responsible for the organization of IT security and carrying out regular meetings of IT security working group.

The **IT Security Officer** is the contact for all employees and contractors and other third parties on issues of IT security and security incidents.

The **executives** create the necessary conditions so that all relevant staff, contractors and other third parties **know, understand and follow** the **information security policy** and the subsequent IT-security concept and its Standard Operating Procedures.

Every **employee** is responsible for compliance with the regulations he is concerned with. Every employee has the responsibility to treat the data created or processed by him accordingly to their purpose and their vulnerability.

3 Protection Goals

All sensitive information, data and IT resources are to be protected in accordance with their vulnerability so that

- only allowed accesses and releases are possible (protection goal: confidentiality);
- only permitted changes are possible (protection goal: integrity);
- only allowed deletions are possible and the systems are permanently available (Protection goal: availability).
- each file and resource can be assigned to their owners and their creators;
- legal, contractual and regulatory requirements can be met.

4 Basic standards

The organization of information security at the **INTERCONTINENTAL® FRANKFURT** is based on the standard ISO / IEC 27001 and the recommendations of ISO 27002. This alignment takes into account the integration of the BSI basic protection in the ISO 27001 framework. The requirements of PCI DSS are implemented and the 'IT Standard Operating Procedure and Best Practices MANUAL" is considered.

5 Information Security Policy / IT Security Concept

The IT security concept concretizes this Information security policy in the following areas:

Classification of data and information, rules for data processing (data collection / capture, store and warehouses , disposal or destruction) and for the permissible use of data and information , human security resources ; Management of security incidents ; physical and environmental security ; Business continuity and disaster recovery ; Ensuring the security of information systems.

6 Standard Operating Procedures (SOPs)

The SOPs describe guidelines and procedures to detect, evaluate and manage the risks of information security in the responsibility of the **INTERCONTINENTAL® FRANKFURT**. We furthermore evaluate the performance of our information security program.

Reports to the hotel management form the basis for regular reviews. This results in preventive and corrective measures in order to achieve a continuous improvement in relation to the risks as well as for the program.

7 IT security and data protection

IT security and data protection are subsets of information security. In these areas, among others apply following guidelines:

We report the IHG immediately unauthorized access to our IT systems and unauthorized access to or unauthorized deletion of personal data.

We may disclose personal data to unauthorized third parties never further and give these also have access to this data.

Frankfurt; in July 2016

The General Manager