

INFORMATIONSSICHERHEITSPOLITIK

Als Royal Group Hotels betrachten wir im Einklang mit unserem innovativen, verlässlichen, nachhaltigen und gästeorientierten Serviceverständnis den Schutz unserer Informationswerte in allen Phasen unserer Tätigkeit als eines der grundlegenden Elemente unserer Unternehmensführung.

Um die Informationen unserer Gäste, Mitarbeitenden, Geschäftspartner, Lieferanten und aller weiteren interessierten Parteien zu schützen, die Informationssicherheit zu einem festen Bestandteil unserer Unternehmenskultur zu machen und unsere Informationssicherheitspraktiken kontinuierlich weiterzuentwickeln, verpflichten wir uns:

- Informationssicherheitsmanagement: unsere Informationssicherheitsprozesse auf Grundlage der Kernprinzipien der Norm ISO/IEC 27001 weiterzuentwickeln sowie technische, physische und organisatorische Maßnahmen zum Schutz unserer Informationswerte einzuführen, umzusetzen und fortlaufend zu verbessern;
- Vertraulichkeit, Integrität und Verfügbarkeit: die Vertraulichkeit, Integrität und Verfügbarkeit unserer Unternehmensinformationen zu wahren und die erforderlichen Sicherheitsmaßnahmen gegen die Risiken von unbefugtem Zugriff, Veränderung, Verlust, Offenlegung und Missbrauch zu ergreifen;
- Risikomanagement: Informationssicherheitsrisiken systematisch zu identifizieren, zu analysieren und zu bewerten, Risikoakzeptanzkriterien und Risikoeigentümer festzulegen, geeignete Maßnahmen zu entwickeln und umzusetzen sowie deren Wirksamkeit regelmäßig zu überwachen;
- Schutz personenbezogener Daten: die personenbezogenen Daten unserer Gäste, Mitarbeitenden und Geschäftspartner im Einklang mit den geltenden Rechtsvorschriften, insbesondere dem türkischen Datenschutzgesetz Nr. 6698 (KVKK), zu verarbeiten, aufzubewahren und zu schützen sowie nach Ablauf der gesetzlichen Aufbewahrungsfristen mit rechtskonformen Verfahren zu vernichten;
- Einhaltung gesetzlicher und vertraglicher Anforderungen: die geltenden nationalen und anwendbaren internationalen Regelungen zur Informationssicherheit, die einschlägigen Rechtsvorschriften, vertragliche Verpflichtungen sowie die Informationssicherheitsanforderungen unserer interessierten Parteien einzuhalten;
- Digitale Sicherheit: die erforderlichen Maßnahmen zur Gewährleistung der Informationssicherheit in Hotelmanagementsystemen, Reservierungsinfrastrukturen, Anwendungen für das Gästebeziehungsmanagement, Zahlungssystemen, Unternehmenskommunikationsnetzen und weiteren digitalen Plattformen zu ergreifen;
- Zugriffsberechtigung: den Zugriff auf Informationswerte entsprechend den jeweiligen Aufgaben, Befugnissen und Verantwortlichkeiten zu beschränken, unbefugte Zugriffe zu verhindern, Zugriffsrechte regelmäßig zu überprüfen und sicherzustellen, dass ausschließlich befugte Personen Zugang zu Informationen erhalten;
- Schutz der Informationswerte: Informationswerte in elektronischer und physischer Form nach ihrem Schutzbedarf zu klassifizieren sowie geeignete Regeln für deren Aufbewahrung, Weitergabe, Übermittlung, Sicherung und sichere Vernichtung festzulegen und anzuwenden;
- Geschäftskontinuität: die möglichen Auswirkungen von Informationssicherheitsbedrohungen auf unsere betrieblichen Prozesse und die Kontinuität unserer Dienstleistungen zu verringern und Maßnahmen zur Unterstützung der Kontinuität kritischer Informationssysteme zu entwickeln;

- Management von Informationssicherheitsvorfällen: mögliche Verletzungen der Informationssicherheit und Cybersicherheitsvorfälle rechtzeitig zu erkennen und zu melden, wirksam auf Vorfälle zu reagieren und Korrekturmaßnahmen zur Vermeidung ihres erneuten Auftretens umzusetzen;
- Sensibilisierung der Mitarbeitenden: sicherzustellen, dass alle Mitarbeitenden ihre Verantwortung für die Informationssicherheit verinnerlichen, und durch Schulungs- und Sensibilisierungsmaßnahmen eine Kultur des sicheren Umgangs mit Informationen zu fördern;
- Sicherheit bei Lieferanten und Geschäftspartnern: die Informationssicherheitspflichten unserer externen Dienstleister, Lieferanten und Geschäftspartner festzulegen und die Einhaltung der jeweiligen Sicherheitsanforderungen zu überwachen;
- Technologische Entwicklung und kontinuierliche Verbesserung: neue Technologien, Prozesse der digitalen Transformation und sich wandelnde Cyberbedrohungen zu verfolgen, um unsere Informationssicherheitspraktiken aktuell zu halten, ihre Leistung zu bewerten und sie kontinuierlich zu verbessern;
- Unternehmensreputation und Vertrauen: durch unsere Informationssicherheitspraktiken das Vertrauen unserer Gäste und aller interessierten Parteien zu bewahren, unsere Unternehmensreputation zu stärken und die Nachhaltigkeit unseres verlässlichen Serviceverständnisses sicherzustellen.

Zu diesen Grundsätzen bekennen wir uns ausdrücklich.

Als oberste Leitung der Royal Group Hotels unterstützen wir die Umsetzung dieser Politik in allen Betrieben, Abteilungen und relevanten Tätigkeitsbereichen der Gruppe, ihre Bekanntmachung gegenüber unseren Mitarbeitenden und relevanten interessierten Parteien, die Bereitstellung der erforderlichen Ressourcen sowie die regelmäßige Überprüfung und kontinuierliche Verbesserung unserer Informationssicherheitspraktiken.