MIRAMARE HOTELS

Informationssicherheitspolitik nach ISO 27001:2022

Diese Informationssicherheitspolitik wurde erstellt, um die Sicherheitsmaßnahmen im Rahmen des Informationssicherheits-Managementsystems (ISMS) der Miramare Hotels festzulegen und die vollständige Einhaltung des ISO 27001:2022-Standards sicherzustellen. Die Richtlinie gilt für alle Mitarbeiter, Lieferanten, Dienstleister und sonstigen relevanten Parteien und umfasst sämtliche Aktivitäten und Datenverarbeitungsprozesse von Miramare Hotels. Miramare Hotels verpflichtet sich, ein ISMS gemäß ISO 27001:2022 aufzubauen, um Risiken im Bereich der Informationssicherheit zu steuern, diese Risiken zu minimieren und eine effektive Sicherheitskultur zu schaffen. Das ISMS enthält alle erforderlichen Verfahren und Kontrollen zur Identifikation, Überwachung und Prüfung wesentlicher Risiken.

Grundsätze der Informationssicherheit:
Miramare Hotels verpflichtet sich zur Einhaltung der folgenden Prinzipien:

- **Vertraulichkeit:** Informationen sind nur für autorisierte Personen zugänglich und werden vor unbefugtem Zugriff Dritter geschützt.
- **Integrität:** Daten dürfen nicht unbefugt verändert werden; Fehler und Manipulationen werden vermieden.
- **Verfügbarkeit:** Autorisierte Personen können jederzeit auf benötigte Informationen zugreifen.

Rechtliche und regulatorische Konformität: Alle Sicherheitsaktivitäten erfolgen in Übereinstimmung mit geltenden Gesetzen und Standards.

Risikomanagement: Miramare Hotels führt kontinuierliche Risikobewertungen aller Informationswerte durch, um potenzielle Bedrohungen und Schwachstellen zu identifizieren. Geeignete Sicherheitsmaßnahmen werden entsprechend implementiert und rege-

lmäßig überprüft.ilerin, yetkili kişiler tarafından her zaman erişilebilir olması sağlanır.

Sicherheitsverletzungen und Vorfallmanagement: Jede Sicherheitsverletzung oder jeder Vorfall wird unverzüglich an das Sicherheitsteam gemeldet. Korrekturmaßnahmen werden getroffen, um Auswirkungen zu minimieren und Wiederholungen zu vermeiden.

Mitarbeiterschulungen und Sensibilisierung: Alle Mitarbeiter werden regelmäßig zu Sicherheitsrichtlinien und bewährten Praktiken geschult. Informationsveranstaltungen erhöhen das Bewusstsein und fördern Verantwortungsbewusstsein im Umgang mit Informationen.

Schutz von Informationswerten: Alle Informationswerte (Daten, Systeme, Infrastruktur etc.) werden sicher verwaltet, nur autorisierte Personen haben Zugriff. Technische und administrative Schutzmaßnahmen wie Verschlüsselung, Backups und Löschprozesse werden implementiert.

Zugriffskontrollen: Zugriffe werden gemäß betrieblichen Erfordernissen gewährt. Rechte werden bei Aufgabenänderungen oder Kündigungen überprüft und angepasst. Zugriffe sind nachvollziehbar und dokumentiert.

Lieferanten- und Drittparteienmanagement: Lieferanten und externe Dienstleister müssen mit den Sicherheitsrichtlinien von Miramare Hotels konform arbeiten. Anforderungen werden vertraglich geregelt.

Kontinuierliche Verbesserung: Das ISMS wird durch interne und externe Audits regelmäßig evaluiert. Korrektur- und Vorbeugemaßnahmen werden bei Bedarf umgesetzt. Die Leistung wird überwacht und dokumentiert.

Überwachung und Audits: Wirksamkeit von Sicherheitsmaßnahmen wird regelmäßig kontrolliert. Bei Abweichungen werden

umgehend Maßnahmen ergriffen.

Überprüfung der Richtlinie: Diese Richtlinie wird regelmäßig überarbeitet und durch die Geschäftsleitung genehmigt, um stets aktuell zu bleiben.

Verantwortlichkeiten: Alle Mitarbeiter, Führungskräfte und Lieferanten tragen Verantwortung für die Informationssicherheit. Verstöße gegen die Richtlinie können disziplinarische Maßnahmen nach sich ziehen. Die Geschäftsführung stellt die Umsetzung und Ressourcen sicher.
Miramare Hotels verpflichtet sich, alle Anforderungen der ISO 27001:2022 zu erfüllen und diese Richtlinie konsequent umzusetzen. Informationssicherheit ist eine unserer höchsten Prioritäten.

GENERAL DIREKTOR