MIRAMARE HOTELS

Политика информационной безопасности ISO 27001:2022

Настоящая политика информационной безопасности разработана для определения мер безопасности в рамках системы управления информационной безопасностью (СУИБ) Miramare Hotels и обеспечения полного соответствия стандарту ISO 27001:2022. Политика распространяется на всех сотрудников, поставщиков, подрядчиков и другие заинтересованные стороны и охватывает всю деятельность и процессы обработки данных компании.
Miramare Hotels обязуется внедрить СУИБ в соответствии со стандартом ISO 27001:2022, управлять рисками информационной безопасности, минимизировать их и создать эффективную культуру информационной безопасности. СУИБ включает все необходимые процедуры и меры контроля для выявления, мониторинга и аудита ключевых рисков.

Принципы информационной безопасности: Miramare Hotels придерживается следующих принципов:

- **Конфиденциальность:** Доступ к информации имеют только уполномоченные лица. Данные защищены от несанкционированного доступа.
- **Целостность:** Изменения данных невозможны без разрешения. Предотвращаются ошибки и искажения.
- **Доступность:** Уполномоченные пользователи всегда имеют доступ к необходимой информации.
- **Соответствие законодательству:** Все действия соответствуют действующим законам и отраслевым стандартам.

Управление рисками: Осуществляется регулярная оценка рисков для всех информационных активов. Реализуются соответствующие меры безопасности и контрольные механизмы. Оценки пересматриваются и обновляются при необходимости.

Инциденты и нарушения: При обнаружении инцидента он немедленно сообщается в команду безопасности. Проводятся корректирующие действия и анализ причин.

Обучение и осведомленность сотрудников: Сотрудники регулярно обучаются политике, процедурам и лучшим практикам. Проводятся информационные кампании для повышения осведомленности.

Защита активов: Все информационные активы (данные, системы и инфраструктура) защищены. Используются методы шифрования, резервного копирования и удаления данных.

Контроль доступа: Доступ предоставляется на основе деловой необходимости. Права доступа пересматриваются при изменении должности или увольнении. Доступ регистрируется и контролируется.

Управление поставщиками и третьими сторонами: Miramare Hotels требует от поставщиков соблюдения политики безопасности. Эти требования закреплены в договорах.

Постоянное улучшение: Система управления информационной безопасностью регулярно оценивается с помощью аудитов. Применяются корректирующие меры. Эффективность системы контролируется и документируется.

Аудит и мониторинг: Меры безопасности оцениваются внутренними и внешними аудитами в соответствии с ISO 27001:2022. Несоответствия устраняются незамедлительно.

Актуализация политики: Политика регулярно пересматривается и обновляется с одобрения высшего руководства.

Ответственность: Все сотрудники, руководители и поставщики несут ответственность за соблюдение политики. Нарушения

влекут дисциплинарные меры. Руководство обеспечивает реализацию и предоставляет ресурсы.
Miramare Hotels подтверждает свою приверженность реализации всех требований ISO 27001:2022. Информационная безопасность — один из наших главных приоритетов.

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР