

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В Royal Group Hotels мы, в соответствии с нашим инновационным, надёжным, устойчивым и ориентированным на гостей подходом к обслуживанию, рассматриваем защиту наших информационных активов на всех этапах деятельности как один из основополагающих элементов корпоративного управления.

В целях защиты информации наших гостей, сотрудников, деловых партнёров, поставщиков и всех других заинтересованных сторон, превращения информационной безопасности в неотъемлемую часть нашей корпоративной культуры и постоянного совершенствования практик информационной безопасности мы обязуемся:

- Управление информационной безопасностью: развивать процессы информационной безопасности на основе ключевых принципов стандарта ISO/IEC 27001, а также создавать, внедрять и постоянно совершенствовать технические, физические и административные меры контроля для защиты информационных активов;
- Конфиденциальность, целостность и доступность: обеспечивать конфиденциальность, целостность и доступность корпоративных информационных активов и принимать необходимые меры безопасности против рисков несанкционированного доступа, изменения, утраты, разглашения и неправомерного использования;
- Управление рисками: систематически выявлять, анализировать и оценивать риски информационной безопасности; определять критерии принятия рисков и владельцев рисков, разрабатывать и внедрять соответствующие меры контроля и регулярно отслеживать их эффективность;
- Защита персональных данных: обрабатывать, хранить и защищать персональные данные наших гостей, сотрудников и деловых партнёров в соответствии с действующим законодательством, прежде всего с Законом Турецкой Республики № 6698 «О защите персональных данных» (KVKK), и уничтожать их по истечении установленных законом сроков хранения способами, соответствующими законодательству;
- Соблюдение правовых и договорных требований: соблюдать действующие национальные и применимые международные нормы в области информационной безопасности, соответствующее законодательство, договорные обязательства и требования заинтересованных сторон в отношении информационной безопасности;
- Цифровая безопасность: принимать необходимые меры для обеспечения информационной безопасности систем управления отелями, инфраструктуры бронирования, приложений для работы с гостями, платёжных систем, корпоративных сетей связи и других цифровых платформ;
- Управление доступом: ограничивать доступ к информационным активам в соответствии с должностными обязанностями, полномочиями и ответственностью; предотвращать несанкционированный доступ, регулярно пересматривать права доступа и обеспечивать доступ к информации только для уполномоченных лиц;
- Защита информационных активов: классифицировать информационные активы в электронной и физической среде по уровню их критичности; устанавливать и применять

надлежащие правила их хранения, совместного использования, передачи, резервного копирования и безопасного уничтожения;

- Непрерывность бизнеса: снижать возможное влияние угроз информационной безопасности на наши операционные процессы и непрерывность обслуживания; разрабатывать меры, поддерживающие непрерывность работы критически важных информационных систем;
- Управление инцидентами информационной безопасности: своевременно выявлять возможные нарушения информационной безопасности и инциденты кибербезопасности и сообщать о них, эффективно реагировать на инциденты и принимать корректирующие меры для предотвращения их повторения;
- Осведомлённость сотрудников: добиваться того, чтобы все наши сотрудники принимали на себя ответственность в области информационной безопасности; развивать культуру безопасного обращения с информацией посредством обучения и мероприятий по повышению осведомлённости;
- Безопасность во взаимодействии с поставщиками и деловыми партнёрами: определять обязательства в области информационной безопасности для наших внешних поставщиков услуг, поставщиков и деловых партнёров и контролировать соблюдение ими соответствующих требований безопасности;
- Технологическое развитие и постоянное совершенствование: отслеживая новые технологии, процессы цифровой трансформации и меняющиеся угрозы кибербезопасности, поддерживать актуальность наших практик информационной безопасности, оценивать их результативность и постоянно их совершенствовать;
- Корпоративная репутация и доверие: благодаря нашим практикам информационной безопасности сохранять доверие гостей и всех заинтересованных сторон, укреплять корпоративную репутацию и обеспечивать устойчивость нашего подхода к надёжному обслуживанию.

Мы подтверждаем свою приверженность изложенным выше принципам.

Мы, высшее руководство Royal Group Hotels, поддерживаем применение настоящей политики на всех объектах, во всех подразделениях и соответствующих сферах деятельности группы, её доведение до сведения сотрудников и заинтересованных сторон, обеспечение необходимых ресурсов, а также регулярный пересмотр и постоянное совершенствование практик информационной безопасности.