

## ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### Наша миссия

Мы, **REGNUM HOTELS**, стремимся защищать конфиденциальность, целостность и доступность данных гостей, персонала, бизнес-процессов и другой чувствительной информации. Мы внедряем лучшие практики для предотвращения утечек данных и развития культуры информационной безопасности, защищая все информационные активы. Наша приоритетная задача – обеспечение доверия клиентов и поддержание непрерывности бизнеса.

### Наша визия

Мы стремимся сделать информационную безопасность неотъемлемой частью всех наших процессов и создать устойчивую культуру безопасности. Работая в условиях защищённой информационной среды, мы стремимся постоянно улучшать качество наших услуг и операций.

### Наши обязательства по информационной безопасности

- Защита информационных активов: Определение, классификация и внедрение мер защиты активов в соответствии с оценкой рисков.
- Обучение и осведомлённость: Проведение регулярного обучения сотрудников по информационной безопасности для повышения уровня осведомлённости и развития культуры безопасности.
- Оценка рисков: Постоянная оценка рисков информационной безопасности и принятие эффективных мер для их предотвращения.
- Мониторинг и улучшение: Регулярный пересмотр, улучшение и аудит наших политик, процессов и контролей для обеспечения соответствия.
- Управление инцидентами: Обнаружение, регистрация, реагирование на инциденты информационной безопасности и уведомление о нарушениях при необходимости.
- Юридическое и регуляторное соответствие: Обеспечение полного соответствия действующим законам, нормативным актам и договорным обязательствам.
- Непрерывность бизнеса: Обеспечение бесперебойного предоставления услуг с помощью эффективных мер информационной безопасности.

Эта политика распространяется на всех сотрудников, стажёров, поставщиков услуг и третьих лиц, использующих информационные системы и ресурсы **REGNUM HOTELS**. Все стороны обязаны соблюдать принципы информационной безопасности и выполнять возложенные на них обязанности в этой области.

Каждый сотрудник несёт ответственность за обеспечение конфиденциальности, целостности и доступности информации. Все работники обязаны соблюдать **Регламент управления персоналом REGNUM HOTELS, Кодекс деловой этики и Закон о защите персональных данных (KVKK)**.



**REGNUM HOTELS** обязуется соблюдать требования KVKK и принимать необходимые меры для защиты персональных данных.

#### **Роли и обязанности**

- Менеджеры по информационной безопасности несут ответственность за реализацию политики, организацию необходимого обучения и руководство процессами информационной безопасности.
- Менеджер IT отвечает за актуализацию политики и создание эффективной системы управления рисками информационной безопасности.
- Руководители отделов обязаны обеспечивать соблюдение политики информационной безопасности в своих подразделениях. В случае несоответствий будут приняты необходимые дисциплинарные меры и, при необходимости, начаты юридические процедуры.

Политика пересматривается не реже одного раза в год и обновляется при необходимости.

Команда по управлению информационной безопасностью контролирует выполнение политики и предоставляет отчёты. Нарушения могут привести к дисциплинарным взысканиям, расторжению трудового договора и юридическим последствиям.

#### **Наши цели**

- Обеспечить непрерывность информационных систем.
- Максимально повысить соответствие требованиям безопасности за счёт повышения осведомлённости сотрудников.
- Обеспечить полное соответствие договорным обязательствам с третьими лицами.
- Предотвращать нарушения информационной безопасности и превращать их в возможности для обучения.
- Создавать, хранить и предоставлять доступ к информации в соответствии с законодательными требованиями.
- Внедрять новейшие технические меры безопасности.

Все сотрудники REGNUM HOTELS несут ответственность за достижение этих целей.