Утверждено
Приказ № 5
от 25 мая 2016г

Положение
Об утверждении политики информационной безопасности для размещения в сети Интернет

1. Общие положения

Обеспечение информационной безопасности является необходимым условием для осуществления деятельности., далее по тексту «Компания». Нарушение информационной безопасности может привести к серьезным последствиям для Компании, включая потерю доверия со стороны клиентов, партнеров, поставщиков и снижение конкурентоспособности.

2. Цель документа

Целью Политики информационной безопасности Компании для размещения в сети интернет (далее - Политика) является декларация основных целей и положений по организации процессов обеспечения и управления информационной безопасностью Компании. Указанная политика предназначена для декларирования подхода Компании к обеспечениюинформационной безопасности. Размещается на сайте Компании в сети интернет для свободного доступа для любого пользователя, кто пожелает с ней ознакомиться.

3. Задачи обеспечения и управления информационной безопасностью

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

Основными задачами в области обеспечения и управления информационной безопасностью Компании являются:

- Обеспечение целостности, доступности и конфиденциальности критичной информации, а также обеспечение доступности критичных ИТ-сервисов Компании;
- Применение обоснованных, экономически эффективных организационных и технических мер по обеспечению информационной безопасности.
- Соответствие Компании требованиям действующего законодательства РФ и регуляторов в области информационной безопасности.
- Соответствие процессов обеспечения информационной безопасности требованиям бизнеса Компании.
- Обеспечение доверия клиентов и партнеров Компании.
- Установление ответственности сотрудников по вопросам обеспечения информационной безопасности и повышение их осведомленности.

3. Подход к обеспечению информационной безопасности

- Информация является важным активом Компании и ее защита является обязанностью каждого сотрудника;
- Доступ к информации предоставляется только лицам, которым он необходим длявыполнения должностных или контрактных обязательств в минимально возможном

объеме;

- Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации;
- Сотрудники Компании проходят регулярное обучение в области информационной безопасности;
- В Компании регулярно проводится независимый аудит информационной безопасности;
- Специалисты информационной безопасности отвечают за определение детальных требований информационной безопасности и контролируют их исполнение в Компании;
- Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности;
- Меры защиты персональных данных внедряются согласно требованиям Федерального закона № 152-ФЗ «О защите персональных данных» и других нормативных документов, регламентирующих обработку персональных данных в автоматизированных и неавтоматизированных информационных системах;
- Оценка рисков информационной безопасности проводится ежегодно, а также в случае значительных изменений в структуре Компании и ее бизнес-процессах;
- При оценке рисков учитывается влияние реализации угроз информационной безопасности на финансовое положение Компании и ее репутацию на рынке;
- Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

4. Порядок изменения политики

Политика должна пересматриваться при наступлении существенных событий, но не реже чем один раз в три года.