УТВЕРЖДЕНО

Распоряжением от 31.08.2015

№ Р-002/2015

**Политика информационной безопасности ИП Воскресенский С. А. для размещения в сети Интернет**

**версия 1.0**

Уровень доступа: общий

Содержание:

*1. Общие положения*

*2. Цели обеспечения и управления информационной безопасностью ООО "Орхидея"*

*3. Подход к обеспечению информационной безопасности*

*4. Порядок пересмотра Политики*

**1. Общие положения**

1.1. Обеспечение информационной безопасности является необходимым условием для осуществления деятельности ИП Воскресенский С.А. (далее - Компания). Нарушение информационной безопасности может привести к серьезные последствиям для Компании, включая потерю доверия со стороны клиентов, партнеров, поставщиков и снижение конкурентоспособности.

1.2. Цель Политики информационной безопасности ИП Воскресенский С.А. для размещения в сети Интернет (далее- Политика) является декларирование основных целей и положений по организации процессов обеспечения и управления информационной безопасностью в Компании.

 1.3. Политика предназначена для опубликования на сайте Компании.

 1.4. Настоящая Политика является общедоступной и предназначена для всех ,кто пожелает ознакомиться с подходом Компании к обеспечению информационной безопасности.

**2.** **Цели обеспечения и управления информационной безопасностью ИП Воскресенский С. А.**

2.1. Основными целями Компании в области информационной безопасности являются:

- обеспечение целостности доступности и конфиденциальности критичной информации;

- применение обоснованных, экономически эффективных организационных и технических мер по обеспечению информационной безопасности;

- соответствие Компании требованиям действующего законодательства и регуляторов в области информационной безопасности;

- соответствие процессов обеспечения информационной безопасности бизнес-требованиям Компании;

- обеспечение доверия клиентов и партнеров Компании;

- установление ответственности сотрудников по вопросам обеспечения информационной безопасности и повышения их осведомленности.

**3. Подход к обеспечению информационной безопасности**

3.1. Информация является активом Компании и ее защита является обязанностью каждого сотрудника.

3.2. Доступ к информации предоставляется только тем лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально необходимом объеме.

3.3. Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

3.4. 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.

3.5. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

**4. Порядок пересмотра Политики**

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