«Утверждаю»

_____

«__» «_____» 20__ г.

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВЗАИМОДЕЙСТВИИ С ВНЕШНИМИ СТОРОНАМИ

Содержание

1 Назначение и область применения

1.1 Процедура описывает действия и меры, направленные на обеспечение информационной безопасности при взаимодействии организации с внешними сторонами (поставщиками, подрядчиками, партнерами и другими заинтересованными сторонами). Цель — минимизация рисков, связанных с утратой конфиденциальности, целостности и доступности информации, а также с угрозами, исходящими от внешних участников.

1.2 Процедура применяется ко всем внешним взаимодействиям, которые включают обмен данными, доступ к информационным системам, а также обработку информации внешними организациями.

2 Нормативные ссылки

2.1 В настоящей документированной процедуре использованы ссылки на следующие нормативные документы:

ISO/IEC 27001:2022	Информационные технологии, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования
ISO/IEC 27002:2022	Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление информационной безопасностью
……..	……
……..	……

3 Термины и определения

Информационная безопасность — защита информации от угроз, которые могут привести к утрате ее конфиденциальности, целостности и доступности.
Внешние стороны — организации или индивидуальные предприниматели, которые предоставляют или получают доступ к информации организации или используют ее в своей деятельности.
Контракт на обработку данных — соглашение между организацией и внешней стороной, регламентирующее использование, обработку и защиту информации.
Риски безопасности информации — вероятность возникновения угроз, которые могут привести к ущербу для организации в случае утраты или несанкционированного доступа к информации.

4 Сокращения и обозначения

ИС — информационная система
СМК — система менеджмента качества
РР — риски безопасности
ДП — договорные положения
ДТ — договор о трансфере данных

5 Ответственность и полномочия

Руководитель службы информационной безопасности (СИБ) отвечает за разработку и внедрение данной процедуры, а также за мониторинг и контроль ее выполнения.
Менеджеры по безопасности обязаны контролировать выполнение требований безопасности при заключении соглашений с внешними сторонами.
Отдел закупок и **Юридический отдел** обеспечивают, чтобы все внешние контракты и соглашения включали положения, направленные на защиту информации.
Все сотрудники должны быть осведомлены о процедурах взаимодействия с внешними сторонами в рамках информационной безопасности.

6 Требования

6.1 Оценка рисков при взаимодействии с внешними сторонами

6.1.1. Перед установлением взаимодействия с внешними сторонами проводится оценка рисков,