**«УТВЕРЖДАЮ»**
Директор
ТОО «Asia Trans KZ»
Воропаева О.Ю.
«25» июля 2023 г.

# Процедура
## по защите данных в цифровом виде

### 1. Цель и область применения

Целью Процедуры является обеспечение надежной защиты конфиденциальной, ценной и чувствительной информации компании, находящейся в цифровом формате. Процедура направлена на минимизацию рисков утечки данных, несанкционированного доступа, вредоносных атак и других угроз, которые могут возникнуть при обработке, хранении и передаче данных о клиентах, продуктах и операциях компании.

### 2. Ответственность

Ответственным за выполнение данной процедуры является: ответственное лицо за направление КЦ.

### 3. Перечень активов информационных технологий и их инвентаризация

- В рамках данной Процедуры создан Перечень активов информационных технологий, включающий как аппаратное обеспечение (десктопы, ноутбуки, планшеты, мобильные телефоны, маршрутизаторы, камеры...), так и программное обеспечение, обрабатывающее информацию.

- Перечень охватывает все устройства и программы, содержащие конфиденциальные данные компании. Инвентаризация проводится для каждого актива, включая определение наименования, модели, серийного номера и других идентификационных данных.

- Эта информация регулярно обновляется, чтобы отразить текущее состояние активов. Инвентаризация также включает активы, находящиеся вне офисных помещений, такие как мобильные устройства. Оборудование и активы вне помещений также подвергаются инвентаризации и мерам защиты.

### 4. Программа упреждающего обслуживания активов информационных технологий

- Для обеспечения надежности и долгосрочной работоспособности активов информационных технологий, работающих с данными, разработана и внедрена программа упреждающего обслуживания. Эта программа основывается на рекомендованных интервалах технического обслуживания, предоставленных поставщиками оборудования и программного обеспечения.

- Программа включает в себя как аппаратное, так и программное обслуживание, чтобы гарантировать оптимальную производительность и безопасность. Записи о проведенных обслуживаниях подробно документируются и заносятся в соответствии с установленными требованиями в Перечень активов ИТ. Это обеспечивает не только планирование и следование регулярному обслуживанию, но и доступ к истории технических мероприятий для каждого актива.

## 5. Аудит информационной системы и соответствие критериям

- С целью обеспечения надежности и соответствия установленным стандартам безопасности, информационная система компании проверяется независимым аудитором не реже одного раза в год.

- Аудит включает оценку выполнения определенных критериев безопасности, установленных в рамках компании и в соответствии с идеологией стандарта ISO 27001.

## 6. Коммуникационный диалог и реагирование на угрозы и инциденты

- Для обеспечения эффективной коммуникации и обмена информацией по вопросам безопасности среди сотрудников и подрядчиков разработана система, предоставляющая информацию о текущих угрозах безопасности, а также обновлений в уровнях угроз: оранжевый (есть подозрения на существование угрозы) и красный (существование угрозы подтверждено).

- В рамках этой системы предоставляется информация как для сотрудников, так и для руководства, чтобы обеспечить адекватную реакцию на изменение ситуации. Также существует система обмена информацией с местными и национальными правоохранительными органами, которая позволяет оперативно реагировать на возможные угрозы.

- Коммуникации, диалог и обмен информацией с заинтересованными сторонами, такими как сотрудники, подрядчики, заказчики, органы власти и другие, осуществляются с соблюдением мер по защите конфиденциальной информации, обеспечивая сбалансированный подход к безопасности и прозрачности.

- В случае возникновения инцидентов незамедлительно проводится оценка ситуации с целью минимизации возможных последствий. Кроме того, создается "культура извлечения уроков" по вопросам защиты данных в цифровом виде внутри компании и, при необходимости, в компаниях-подрядчиках, что позволяет улучшать практики и предотвращать подобные инциденты в будущем.

## 7. Управление рисками

- Периодическая оценка рисков проводится не реже одного раза в двенадцать месяцев. Оценка рисков охватывает данные о клиентах, продуктах и операциях компании и включает идентификацию потенциальных угроз и уязвимостей в системе хранения и обработки данных.

- Компания использует меры защиты данных, обработку заказов и использование данных о заказах клиентов на корпоративном интернет-сайте. Система электронного обмена данными настроена для безопасной передачи деловых документов между компьютерами в стандартном электронном формате. Инструменты обработки заказов настроены с учетом защиты данных, чтобы предотвратить несанкционированный доступ и утечку информации.

- Риски, связанные с защитой данных, включают, как минимум:
  - Хакерские атаки, включая попытки несанкционированного доступа к системам.
  - Распространение инфекционного вредоносного программного обеспечения (ПО).
  - Недостаточная безопасность деловой информации на ноутбуках, планшетах, сотовых телефонах и других мобильных устройствах.

- Для снижения рисков хакерских атак, компания использует меры аутентификации, и контролирует доступ к чувствительным данным. Для предотвращения распространения инфекционного ПО, регулярно обновляется антивирусное программное обеспечение, отслеживается сетевая активность и предоставляется обучение сотрудникам по опознанию вредоносных вложений, а также по правилам безопасности при работе с мобильными устройствами.

- Управление рисками при выполнении защиты данных в цифровом виде осуществляется в соответствии с Процедурой идентификации, оценки и приоритизации рисков [2023-Пр-ИОП-Д-01] и Картой Риска, указанной в Приложении №1 к данной Процедуре.

- Каждый “Сценарий реагирования при наступлении рискового события” Таблицы №2 Карты Риска предполагает обязательное выполнение стандартных требований:
  - *Сообщить своему руководителю о несоответствии (см. Политику ОН),*
  - *Сообщить грузоотправителю/заказчику о несоответствии,*
  - *Зафиксировать несоответствие в Журнале Отчетности о Несоответствиях (ЖОН)*
  - *Провести расследование инцидента, используя отраслевые рекомендации, стандарты и правила,*
  - *Исходя из результатов расследования инцидента, провести необходимое специальное обучение ответственных лиц с проверкой знаний*

## 8. Обучение сотрудников

- Обучение персонала: Проводить регулярное обучение персонала по правилам защиты и действиям в случае возникновения угроз утечки данных, несанкционированного доступа, вредоносных атак и других угроз, которые могут возникнуть при обработке, хранении и передаче данных о клиентах, продуктах и операциях компании. За

соответствующее обучение сотрудников компании отвечает: ответственное лицо за направление КЦ.

- Ответственные лица транспортных компаний-подрядчиков должны быть обучены данной Процедуре и инструкциям по защите данных в цифровом виде. За соответствующее обучение ответственных лиц транспортных компаний-подрядчиков отвечает:ответственное лицо за направление ОД.

## 9. Обзор и обновление Процедуры

- Процедура регулярно рассматривается и обновляется по мере необходимости, с учетом возможных изменений и обновлений в требованиях защиты данных в цифровом виде, а также в случае появления новых требований или законодательства, связанного с данной сферой.

## 10. Используемые отраслевые рекомендации, стандарты и правила

- 2013, CEFIC, Responsible Care, “Responsible Care Security Code Guidance and Best Practice for the Implementation of the Code”

## ИЗМЕНЕНИЯ

| № п/п | Версия | Статус документа | Разработчик документа | | Дата разработки |
|---|---|---|---|---|---|
| | | | Должность | Ф.И.О. | |
| 1 | 1 | Действующий. Пересмотр запланирован на декабрь 2023 | Логист | Воропаев А.Ю. | 25.07.2023 |

## ЛИСТ ОЗНАКОМЛЕНИЯ

| № п/п | Должность | ФИО | Подпись | Дата |
|---|---|---|---|---|
| 1 | Директор | Воропаева Олеся Юрьевна | | 25.07.23 |
| 2 | Зам. директора | Хен Андрей Владимирович | | 25.07.23 |
| 3 | Логист | Боденов Сергей Юрьевич | | 25.07.23 |
| 4 | Логист | Анцев Сергей Сергеевич | | 25.07.23 |
| 5 | Логист | Работягова Марина Александровна | | 25.07.23 |
| 6 | Логист | Долидчик Алёна Игоревна | | 25.07.23 |
| 7 | Логист | Кравцов Денис Вячеславович | | 25.07.23 |

**ПРИЛОЖЕНИЕ №1**

# КАРТА РИСКА № 2023-КР-ЗДЦВ-КЦ-01

1. Дата разработки: «30» июля 2023 г.
2. Карту Рисков разработал: /Логист/Воропаев А.Ю./_____
3. Таблица 1: Качественный анализ (матрица риска А*В)

| Тяжесть последствий (А) | | Вероятность инцидента - рискового события (В) | | | |
|---|---|---|---|---|---|
| | | Мало вероятен | Умеренно вероятен | Высоко вероятен | Крайне высоко вероятен |
| | | 1 | 2 | 3 | 4 |
| Крайне высокие последствия | 4 | Риск №1 | Риск №4 | Риск №5 | |
| Высокие последствия | 3 | | | Риск №3 | |
| Умеренные последствия | 2 | | | Риск №2 | |
| Малые последствия | 1 | | | | |

4. Таблица 2: Сценарии реагирования и упреждающие действия

| | Описание риска | (А) | (В) | (А*В) | Сценарии реагирования при наступлении рискового события* | Упреждающие действия для предотвращения рискового события |
|---|---|---|---|---|---|---|
| 1 | *Хакерские атаки, включая попытки несанкционированного доступа к системам* | *4* | *1* | *4* | *Изолировать инфицированные системы, восстановить данные и системы, установить обновления и патчи, выполнить стандартные требования (см. п.7 Процедуры)* | *Регулярно проводить обновления ПО, установить сильные пароли и обеспечить 2FA/3FA, ввести разные уровни доступа* |
| 2 | *Распространение инфекционного вредоносного программного обеспечения* | *2* | *3* | *6* | *Изоляция инфекции и отключение, сканирование зараженных систем и удаление, восстановление данных, выполнить стандартные* | *Установка антивирусного ПО и обновление, фильтрация трафика и брандмауэры, резервное копирование данных* |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | *требования (см. п.7 Процедуры)* | |
| 3 | *Недостаточная безопасность деловой информации на ноутбуках, планшетах, сотовых телефонах и других мобильных устройствах* | *3* | *3* | *9* | *Изоляция устройства, дистанционное удаление данных, смена паролей, выполнить стандартные требования (см. п.7 Процедуры)* | *Шифрование данных на уровне устройства, строгая политика безопасности устройств, дистанционное управление устройствами, установка антивирусного ПО* |
| 4 | *Фишинг и социальная инженерия - атаки, направленные на обман сотрудников и пользователей* | *4* | *2* | *8* | *Определить объем скомпрометированных данных и уведомить о возможных последствиях, выполнить стандартные требования (см. п.7 Процедуры)* | *Внедрить системы многофакторной аутентификации 2FA/3FA для доступа к важным системам и данным, использовать надежное антивирусное ПО и специализированные антиспам-фильтры* |
| 5 | *Несоответствие нормативным требованиям общего регламента по защите персональных данных GDPR* | *4* | *3* | *12* | *Приостановить все процессы и операции, которые нарушают нормативные требования GDPR. Это может включать в себя приостановку обработки определенных видов персональных данных или ограничение доступа к определенным системам, выполнить стандартные требования (см. п.7 Процедуры)* | *Провести обучение сотрудников, особенно тех, которые работают с персональными данными, о требованиях и принципах GDPR, при работе с внешними поставщиками или партнерами, обрабатывающими персональные данные, предусмотреть обязательства по соблюдению GDPR* |

5. *Возможные экстренные меры:
   - В случае наступления рискового события с возможными высокими последствиями, обратиться за содействием к государственным службам

6. Утвердить Карту Риска: _____/Воропаева О.Ю./