«СИЛЛЕНО»
ЖАУАПКЕРШІЛІГІ
ШЕКТЕУЛІ СЕРІКТЕСТІГІ

SILLENO

ТОВАРИЩЕСТВО С
ОГРАНИЧЕННОЙ
ОТВЕТСТВЕННОСТЬЮ
«СИЛЛЕНО»

БҰЙРЫҚ **ПРИКАЗ**

_____№_____

Астана қаласы город Астана

Об утверждении
Политики информационной безопасности

В целях обеспечения сохранности служебной и коммерческой тайны для предотвращения рисков распространения конфиденциальной информации и определения мероприятий, процедур, инструкций и правил по защите информационных систем ТОО «Силлено» (далее – Товарищество), **ПРИКАЗЫВАЮ:**

1. Утвердить Политику информационной безопасности Товарищества, согласно приложению к настоящему приказу.
2. Обратить внимание всех работников Товарищества на необходимость неукоснительного соблюдения Политики информационной безопасности Товарищества по неразглашению информации, содержащей служебную и коммерческую тайну Товарищества.
3. Директору департамента закупок и административной работы (Балашова Л.П.) обеспечить ознакомление работников Товарищества с данной Политикой.
4. Настоящий приказ вступает в силу со дня подписания.

Генеральный директор **Ж.А. Қайргелді**

Исп. М.Г. Есимов
тел.: 64 83 90

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТОО СИЛЛЕНО

г. Астана, 2023 год

Разработал: Главный специалист по информационной безопасности М. Есимов	Проверил: Директор Департамента закупок и административной работы Л. Балашова	Утвержден приказом Генерального директора

Содержание

1. ВВЕДЕНИЕ

1.1. Политика информационной безопасности (далее - Политика) предназначена для определения целей и требований обеспечения информационной безопасности.

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 пользователям, целостность - в случае внесения в данные исключительно авторизованных изменений, доступность - обеспечение возможности получения доступа к данным авторизованным пользователям в нужное для них время.

1.2. Политика информационной безопасности в ТОО «Силлено» (далее Компания) определяет мероприятия, процедуры, инструкции и правила по защите информации в информационных системах ТОО «Силлено».

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Настоящая Политика распространяется на всех работников Компании, имеющих доступ к ее информационным активам, а также на третьих лиц, оказывающих Компании услуги в соответствии с заключенными договорами, и является обязательной для исполнения.

2.2. Настоящая Политика применима ко всей компьютерной технике, сетям, приложениям, автоматизированным и информационным системам Компании, а также к процессам администрирования, сопровождения и использования информационных систем Компании.

2.3. Положение настоящей Политики распространяется на сотрудников Компании и к конфиденциальной информации (защищаемой информации) Компании, в том числе на:

- персональные данные работника в соответствии с законодательством Республики Казахстана о персональных данных и их защите;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией;
- служебные сведения, доступ к которым ограничен органами государственной власти;
- сведения, связанные с коммерческой деятельностью Компании;
- конфиденциальная информация, доступ к которой получен при исполнении обязанностей по трудовому договору;
- информация, составляющая коммерческую тайну и служебную информацию (техническую, коммерческую, юридическую или какого-либо иного характера) Компании и/или его партнеров/клиентов/контрагентов/аффилированных Компании юридических лиц (далее – Конфиденциальная информация), которая доверена или станет известна в процессе исполнения должностных обязанностей.

3. ЦЕЛЯМИ НАСТОЯЩЕЙ ПОЛИТИКИ

3.1. Обеспечение конфиденциальности, целостности, доступности защищаемой информации.

3.2. Предотвращение утечек защищаемой информации.

3.3. Мониторинг событий безопасности и реагирование на инциденты безопасности.

3.4. Нейтрализация актуальных угроз безопасности информации.

3.5. Выполнение требований действующего законодательства по защите информации.

3.6. Выполнение требований действующего законодательства о персональных данных и их защите.

3.7. Политика соответствует международному стандарту ISO/IEC 27001:2015 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

4. ПРИНЦИПЫ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

4.1. Защита конфиденциальности данных должна обеспечивать защиту конфиденциальности информации, особенно относящейся к коммерческим сделкам, стратегическим планам и техническим данным. Это может включать установку механизмов контроля доступа, шифрования данных и усиленную защиту персональной информации.

4.2. Обеспечение целостности данных должна гарантировать, что данные, хранящиеся и передаваемые внутри Компании, не подвергаются несанкционированным изменениям или повреждениям. Это достигается путем применения методов аутентификации и цифровой подписи, а также регулярного мониторинга и аудита систем.

4.3. Защита от кибератак: стратегия по защите от кибератак, включающую меры по предотвращению, обнаружению и реагированию на инциденты. Это может включать использование современных средств защиты, таких как межсетевые экраны, системы обнаружения вторжений и защиту от вредоносных программ.

4.4. Обучение и осведомленность: проводить регулярные обучающие программы и мероприятия для своих сотрудников, направленные на повышение осведомленности о информационной безопасности. Это может включать обучение по распознаванию фишинговых атак, правилам использования паролей, безопасному обращению с электронной почтой и другим аспектам безопасного использования информационных систем.

4.5. Резервное копирование и восстановление: процедуры и системы для резервного копирования данных и восстановления информационных систем в случае чрезвычайных ситуаций или инцидентов. Регулярное создание резервных копий и тестирование процедур восстановления.

5. НЕШТАТНЫМИ СИТУАЦИЯМИ ЯВЛЯЮТСЯ

5.1. Разглашение информации ограниченного доступа сотрудниками Компании, имеющими к ней право доступа, в том числе:

- разглашение информации лицам, не имеющим права доступа к защищаемой информации;
- передача информации по незащищенным каналам связи;
- обработка информации на незащищенных технических средствах обработки информации;
- опубликование информации в открытой печати и других средствах массовой информации;

- передача носителя информации лицу, не имеющему права доступа к ней;
- утрата носителя с информацией.

5.2. Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное изменение информации;
- несанкционированное копирование информации;
- несанкционированные раскрытие информации;

5.3. Несанкционированный доступ к защищаемой информации:

- несанкционированное подключение технических средств к средствам и системам защищаемой информации;
- использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам Компании;
- использование злоумышленником уязвимостей программного обеспечения;
- использование злоумышленником вредоносных программ;
- заражение информационных систем злоумышленником программными вирусами;
- хищение носителей информации;
- нарушение функционирования технических средств обработки информации;
- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

5.4. дефекты, сбои, отказы, аварии технических средств и информационных систем.
5.5. дефекты, сбои, отказы программного обеспечения.
5.6. природные явления, стихийные бедствия:

- термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
- механические факторы (повреждения зданий, землетрясения и т. д.);
- электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

5.7. В случае возникновения нештатной ситуации порядок действий, при которой не регламентирован настоящей Политикой, ответственный за информационные технологии и ответственный за информационную безопасность вырабатывают конкретный план действий с учетом текущей ситуации.

5.8. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 1 к настоящей Политике информационной безопасности.

5.9. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

5.10. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, выполняются действия в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

5.11. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств, а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, ответственный за информационные технологии восстанавливает их из резервных копий.

5.12. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- пользователи корректно отключают и обесточивают свои рабочие места;
- ответственный за ИТ корректно отключает и обесточивает серверы и сетевое оборудование;
- ответственный за ИТ предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, ответственный за ИТ восстанавливает их из резервных копий;
- в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.