SAMRUK-KAZYNA
ONDEU

ТОО «SK Ondeu»

Департамент корпоративной, производственной безопасности и охраны окружающей среды

ПРИЛОЖЕНИЕ № 1
К ПРОТОКОЛУ ЗАСЕДАНИЯ ПРАВЛЕНИЯ
ОТ 14 марта 2024 ГОДА № 05/24

Политика информационной безопасности ТОО «SK Ondeu»

Владелец документа

Ф.И.О.	Петровский Евгений Владимирович
Подразделение	Департамент корпоративной, производственной безопасности и охраны окружающей среды
Должность	Старший менеджер по информационной безопасности
Ф.И.О. непосредственного руководителя	
Должность непосредственного руководителя	Директор департамента

Контроль версий

Номер	Статус	Дата	Автор	Описание изменений
1.0	Активный	30.09.2020 г.	Петровский Е. В.	Первая редакция
2.0	Активный	13.03.2024 г.	Петровский Е. В.	Пересмотр редакции: Обозначение области действия СУИБ, добавление структуры СУИБ, дополнение и изменение ВД составляющих СУИБ, изменения согласно штатному расписанию.

СОДЕРЖАНИЕ

1. СТАТУС ДОКУМЕНТА

1.1 Политика информационной безопасности ТОО «SK Ondeu» (далее - Политика) является документом верхнего уровня согласно иерархии внутренних документов ТОО «SK Ondeu» (далее - Товарищество), неотъемлемой составной частью концепции развития системы управления информационной безопасностью (далее - СУИБ) и определяет основные принципы и задачи функционирования СУИБ.

1.2 Областью действия СУИБ являются значимые для Товарищества Активы. СУИБ Товарищества создается в виде четырехуровневой системы документированных политик, правил, процедур, практических приемов или руководящих принципов, которыми руководствуется Товарищество:

- Политика информационной безопасности является документом первого уровня и определяет цели, задачи, руководящие принципы и практические приемы в области обеспечения ИБ;

- документы второго уровня детализируют требования Политики (политики, методики, правила);

- документы третьего уровня содержат описание процессов и процедур обеспечения ИБ (реестры, планы, регламенты, инструкции);

- документы четвертого уровня включают рабочие формы, журналы, заявки, протоколы и другие документы, в том числе электронные, используемые для регистрации и подтверждения выполнения процедур и работ.

1.3 Целью политики является обеспечение оптимального уровня безопасности Активов Товарищества, согласно стратегии, бизнес-целей, планов и задач, поддержание непрерывности бизнеса, предупреждение возникновения угроз и минимизация влияния внешних угроз финансовой стабильности, рентабельности и положительной репутации Товарищества.

1.4 Политика является основой для защиты информационных Активов Товарищества в разрезе их конфиденциальности, целостности, доступности.

1.5 Положения Политики детализируются в низших по иерархии внутренних документах Товарищества, вводятся в действие и пересматриваются в соответствии с установленным в них порядке.

1.6 Действие Политики распространяется на информационные Активы Товарищества и бизнес-процессы, в которых они задействованы, работников Товарищества, отношения Товарищества с третьими лицами, предоставляющими Товариществу услуги, а также деловых партнеров и контрагентов, имеющим доступ к информационным Активам Товарищества.

1.7 Политика и ниже по иерархии внутренние документы Товарищества доступны для работников Товарищества в пределах их полномочий и предназначены способствовать выполнению ими требований информационной безопасности.

Политика обязательна для выполнения всеми структурными подразделениями и работниками Товарищества. За нарушение требований Политики работники Товарищества несут дисциплинарную ответственность и ответственность, предусмотренную действующим законодательством Республики Казахстан.

1.8 Политика разработана в соответствии с международным и Государственным стандартами в области информационной безопасности ISO 27001 и требованиям законодательства Республики Казахстан, а именно:

- Закон Республики Казахстан «О национальной безопасности Республики Казахстан»;
- Закон Республики Казахстан «Об информатизации»;
- Закон Республики Казахстан «О персональных данных и их защите»;
- Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи»;
- постановление Правительства Республики Казахстан «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

2. ОПРЕДЕЛЕНИЕ ТЕРМИНОВ

2.1. Для целей настоящей Политики используются следующие определения:

1) **Информационный Актив (Актив)** - совокупность данных (сведений), что составляет ценность для Товарищества, а также любая система обработки, обмена или физического места хранения такой информации;

2) **Информационная безопасность (ИБ)** - совокупность процессов и мероприятий, имеющих целью обеспечение целостности, конфиденциальности, доступности информации;

3) **Информационная система (ИС)** - организационно-техническая система, в которой реализуется технология обработки информации с использованием технических и программных средств;

4) **Инцидент информационной безопасности (инцидент ИБ)** - нежелательное или непредвиденное событие информационной безопасности (или их серия), в результате которой может произойти нарушение заложенных механизмов информационной безопасности и/или компрометация информационного Актива Товарищества;

5) **Система управления информационной безопасностью (СУИБ)** - часть общей системы менеджмента Товарищества, основанной на подходе, учитывающем бизнес-риски, предназначенная для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и модернизации информационной безопасности;

6) **Товарищество** - ТОО «SK Ondeu»;

7) **Угроза** - потенциальная причина нежелательного инцидента, который может нанести ущерб Активам, информационным системам Товарищества или Товариществу в целом;

8) **Уязвимость** - слабость актива (группы активов) из-за отсутствия, недостаточности мер и механизмов безопасности, в результате эксплуатации которой возможна компрометация Актива.

2.2. Другие термины и сокращения в Политике используются в значении, изложенном в международном стандарте ISO\IEC 27000.

3. ОСНОВНЫЕ ПРИНЦИПЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1 Основными принципами, которые обеспечивают ИБ информационных Активов Товарищества является:

- ***защищенность:*** поддержание надлежащего уровня защиты Активов с обеспечением целостности, конфиденциальности, доступности;
- ***законность:*** СУИБ Товарищества принимает во внимание требования действующего законодательства Республики Казахстан, а также международной нормативной базы в области информационной безопасности. Товарищество обеспечивает выполнение всех требований по информационной безопасности, имеющиеся в сделках с третьими сторонами;
- ***согласованность и целостность:*** цели и задачи информационной безопасности Товарищества должны соответствовать стратегическим целям и текущим задачам Товарищества, в том числе и тем, которые связаны с внедрением новых бизнес-процессов/продуктов с использованием новейших технологий. Управление информационной безопасностью является неотъемлемой частью управления Товариществом;
- ***эффективность:*** механизмы защиты информационных Активов должны быть адекватными и эффективными с точки зрения минимизации рисков. Товарищество поддерживает риск-ориентированный подход, который обеспечивает понимание, мониторинг и уменьшение рисков операционной деятельности Товарищества;
- ***практичность:*** механизмы защиты информационного Актива должны быть практичными и иметь цель достижения баланса между работоспособностью ресурса и его защищенностью;
- ***непрерывность:*** ИБ представляет собой непрерывный процесс противостояния угрозам и управления рисками информационной безопасности, характерными для сферы деятельности Товарищества;
- ***ответственность:*** каждый Актив Товарищества имеет назначенного владельца, ответственного за нарушение требований ИБ и их последствия; руководство Товарищества всех уровней, работники, бизнес-партнеры и другие стороны, связанные с предоставлением услуг Товариществу должны придерживаться внутренних документов информационной безопасности Товарищества и нести персональную ответственность за их несоблюдение;
- ***опытность***: пользователи информационных Активов Товарищества должны иметь необходимый и достаточный опыт для работы с ними;
- ***прозрачность***: требования ИБ должны быть прозрачными и доступными для владельцев и пользователей информационных Активов Товарищества;
- ***минимальность полномочий:*** доступ к информационным Активам предоставляется в минимально необходимом объеме для выполнения служебных обязанностей.

3.2 Принципы ИБ Товарищества должны быть интегрированы во все аспекты управления бизнес-процессами и информационными технологиями.

3.3 Основными задачами ИБ Товарищества являются:

- управление ИБ, в том числе определение ролей и ответственности в области ИБ;
- классификация Активов;
- оценка рисков ИБ критических бизнес-процессов Товарищества;
- обеспечение безопасности Активов в соответствии с их классификацией, а также оценкой рисков;
- мониторинг событий ИБ, а также управления инцидентами ИБ;
- непрерывность деятельности Товарищества.

3.4 С целью обеспечения функционирования информационных систем в случае возникновения чрезвычайных ситуаций в Товариществе разрабатываются, внедряются, тестируются и обновляются Планы обеспечения непрерывной деятельности и действий в случае возникновения чрезвычайных ситуаций на случай непредвиденных критических ситуаций.

4. ПОДДЕРЖКА И ОТВЕТСТВЕННОСТЬ РУКОВОДСТВА ТОВАРИЩЕСТВА

4.1 Правление Товарищества осознает важность СУИБ для жизнедеятельности Товарищества и демонстрирует свое стремление всесторонне способствовать ее развитию за счет:

4.1.1 обеспечения совместимости политики и целей ИБ со стратегическими задачами Товарищества;

4.1.2 обеспечения интеграции требований СУИБ в бизнес-процессы Товарищества;

4.1.3 обеспечения доступности необходимых для организации СУИБ ресурсов;

4.1.4 информирования работников Товарищества о важности выполнения требований и обеспечения результативности СУИБ;

4.1.5 обучения работников знаниям в области ИБ для повышения эффективности СУИБ.

4.2 Руководство обеспечивает постоянное развитие и повышение квалификации персонала, ответственного за ИБ Товарищества, в том числе прохождение специализированных курсов в сфере обеспечения ИБ не реже одного раза в три года с выдачей сертификата.

4.3 Как владелец информационных Активов и ресурсов Товарищества, Правление Товарищества несет ответственность за управление рисками ИБ и за выбранные меры их обработки (принятие, минимизация, ликвидация, передача третьим лицам).

4.4 Правление Товарищества должно проводить периодический анализ ИБ с точки зрения эффективности, адекватности и результативности, включая:

4.4.1 статус действий по результатам предыдущих проверок;

4.4.2 изменение внешних и внутренних аспектов, имеющих отношение к ИБ;

4.4.3 обратную связь с ответственным за направление ИБ;

4.4.4 возможность дальнейшего развития и совершенствования.

5. РОЛИ И ОТВЕТСТВЕННОСТЬ

5.1. Для обеспечения эффективной системы ИБ Товарищества нужна активная поддержка и непрерывное участие работников различных структурных подразделений на всех уровнях управления.

5.2. Распределение ролей и определение ответственности руководства Товарищества и структурных подразделений Товарищества в функционировании СУИБ Товарищества приведены в Таблице 1 к настоящей Политике.

Таблица 1

роль	Ответственный	Характеристика и ответственность
Управленческая, Владелец бизнес-процесса Товарищества	Руководство Товарищества	▪ периодический анализ ИБ; ▪ формулировка принципов и задач ИБ - основы жизнедеятельности Товарищества; ▪ принятие решений по управлению рисками ИБ; ▪ предоставление необходимых и достаточных ресурсов (включая персонал и финансовые ресурсы) для внедрения СУИБ; ▪ содействие в расследовании инцидентов ИБ; ▪ создание условий для систематического обучения нормам и мерам ИБ с целью уменьшения рисков возникновения инцидентов ИБ;
Распорядитель СУИБ, координатор проектов ИБ Товарищества, контролёр	Управление ИБ	▪ разработка Политики информационной безопасности и внутренних документов по вопросам ИБ; ▪ утверждение плана обработки рисков ИБ; ▪ непосредственное участие и координация проектов ИБ Товарищества; ▪ контроль состояния защиты информационных Активов Товарищества, подготовка соответствующих отчетов Руководству Товарищества; ▪ оценка рисков ИБ; ▪ мониторинг и просмотр рисков и процесса управления рисками ИБ; ▪ выбор механизмов защиты информационных Активов - как организационных мер, так и технических средств (вместе с подразделением информационных технологий); ▪ разработка, внедрение и контроль за выполнением требований ИБ работниками Товарищества; ▪ периодический мониторинг уязвимостей ИС Товарищества;

		▪ контроль за предоставлением и периодический анализ прав доступа пользователей к ИС Товарищества; ▪ мониторинг событий ИБ; ▪ управление инцидентами ИБ; ▪ анализ текущих и планируемых изменений в ИС с точки зрения ИБ; ▪ осуществление контроля за всеми видами информации с точки зрения обеспечения ее целостности, конфиденциальности, доступности, согласно требованиям владельцев бизнес-процессов, внешних регуляторов и лучших международных практик в области ИБ.
Исполнитель	Исполнитель функционала ИТ	▪ участие в проведении оценки рисков ИБ; ▪ участие в выборе механизмов защиты информационных Активов - как организационных мер, так и технических средств; ▪ внедрение и администрирование технических средств защиты информационных Активов; ▪ предоставление / изменение / отмена прав доступа пользователей к информационным системам; ▪ участие в процессе расследования инцидентов ИБ; ▪ управление жизненным циклом ИС; ▪ обеспечение функционирования информационных Активов в случае возникновения чрезвычайных ситуаций.
Исполнитель	Конечные пользователи	▪ непосредственное соблюдение требований ИБ Товарищества; ▪ поддержка соответствующего уровня ИБ Товарищества, в пределах своих служебных обязанностей и полномочий; ▪ содействие в предупреждении инцидентов ИБ.
Контролёр	Структурное подразделение ответственное за риски	▪ участие в разработке методики оценки информационных рисков; ▪ участие в процессе оценки рисков информационной безопасности.
Контролёр	Внутренний аудит	▪ предоставление руководству Товарищества отчета, по контролям функций ИБ.
Контролёр	Внешний аудит	▪ предоставление руководству Товарищества независимых, объективных оценок достаточности и эффективности ИБ.

6. СОСТАВЛЯЮЩИЕ ЧАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТОВАРИЩЕСТВА

6.1 Детализация Политики реализуется в следующих, ниже по иерархии, внутренних документах Товарищества:

- Методика оценки рисков информационной безопасности ТОО «SK Ondeu»;
- Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации ТОО «SK Ondeu»;
- Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации ТОО «SK Ondeu»;
- Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения ТОО «SK Ondeu»;
- Правила использования средств криптографической защиты информации ТОО «SK Ondeu»;
- Правила разграничения прав доступа к электронным информационным ресурсам ТОО «SK Ondeu»;
- Правила использования сети Интернет и электронной почты ТОО «SK Ondeu»;
- Правила организации антивирусного контроля ТОО «SK Ondeu»;
- Правила использования мобильных устройств и носителей информации ТОО «SK Ondeu»;
- Программа обучения пользователей информационной безопасности ТОО «SK Ondeu»;
- Правила проведения внутреннего аудита ИБ ТОО «SK Ondeu».

6.2 В состав СУИБ также входят: процедуры, регламенты, реестры, инструкции и другие внутренние документы по информационной безопасности ТОО «SK Ondeu».

6.3 Политика реализуется в комплексе мероприятий по обеспечению технической, программной и криптографической защиты информации в системах информатизации и связи.

6.4 Разработанный комплект внутренних документов, доступный работникам Товарищества в пределах их полномочий направлен на реализацию мер безопасности для защиты ресурсов СУИБ от угроз. Порядок и режим доступа сотрудников Товарищества к внутренним документам по ИБ, содержащих информацию с ограниченным доступом, определяется в зависимости от их функциональных обязанностей.

7. СТРАТЕГИЯ РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1 Стратегия Товарищества по поддержке и развитию ИБ предусматривает приоритеты реализации наиболее важных и актуальных направлений обеспечения ИБ, с учетом предоставленных финансовых ресурсов.

7.2 Стратегия ИБ предусматривает комплексное развитие путем:

- централизации и единого комплексного подхода к решению всех задач информационного обеспечения и ИБ Товарищества в целом;

- интегрирования всех ключевых направлений задач информационного обеспечения и автоматизации деятельности;
- использования лучших образцов мирового и отечественного опыта, современного технического оборудования и средств программного обеспечения;

8. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1 Внешний независимый аудит информационной безопасности, тесты на проникновение, сканирование на уязвимости проводятся не реже одного раза в два года, или в случае необходимости, с предоставлением раскрытого отчета тестов и аудита.

8.2 Внутренний аудит проводится согласно внутренним документам Товарищества.

9. ПЕРЕСМОТР ПОЛИТИКИ

9.1. Политика, вступает в силу после ее утверждения Правлением Товарищества и действует до ее отмены, изменения или утверждения Правлением Товарищества Политики в новой редакции, со вступлением в силу которой предыдущая теряет силу.

9.2. Изменения и дополнения к настоящей Политики вносятся путем их утверждения Правлением Товарищества.

9.3. Политика пересматривается по мере необходимости, но не реже одного раза в 2 года. Причинами внесения изменений в Политики, могут быть изменения глобальной стратегии Товарищества, изменения в организационной структуре, а также изменения в законодательных, регуляторных и других нормах, которые могут существенно повлиять на распределение ролей и обязанностей по ИБ.