	ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТОВАРИЩЕСТВА (Г-П-Корп-02) **Редакция 1**	

1.ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1 Назначение: Политика информационной безопасности (далее –Политика) устанавливает цели, задачи и подходы в области информационной безопасности.

1.2 Область применения: Товарищество с ограниченной ответственностью «Топливно-энергетический комплекс-КАЗАХСТАН и Товарищество с ограниченной ответственностью «Торговый дом «Топливно-энергетический комплекс – КАЗАХСТАН» (далее – Товарищество) осуществляют деятельность в сфере оказания услуг, связанных с транспортировкой, приемом, хранением и отпуском нефтепродуктов.

Осуществление указанной деятельности связано с управлением информацией, являющейся важным активом, и зависит от обеспечения информационной безопасности, под которой понимается обеспечение конфиденциальности, целостности и доступности информационных активов.

Политика является обязательной для ознакомления и применения всеми структурными подразделениями и всеми работниками Товарищества с ограниченной ответственностью «Топливно-энергетический комплекс – КАЗАХСТАН» и Товарищества с ограниченной ответственностью «Торговый дом «Топливно-энергетический комплекс – КАЗАХСТАН», а также их органами управления, согласно Уставам.

Действие настоящей Политики распространяется на все виды деятельности Товарищества с ограниченной ответственностью «Топливно-энергетический комплекс – КАЗАХСТАН» и Товарищества с ограниченной ответственностью «Торговый дом «Топливно-энергетический комплекс – КАЗАХСТАН».

2. ССЫЛКИ НА ДОКУМЕНТЫ

2.1 Стандарт СТ РК ГОСТ Р ИСО/МЭК 15408 - Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий
2.2 Политика Товарищества по противодействию коррупции и мошенничеству **(Г-П-ДЭБ-01);**
2.3 Положением о конфиденциальной информации **(П-ЮД-03)/(П-03);**
2.4 Инструкция о порядке доступа в серверные помещении **(РИ-ДПИТ-04);**
2.5 Инструкция о правилах управления рисками Товарищества **(Г-РИ-Корп-01);**
2.6 Доступ к ресурсам автоматизированной системы **(Г-РИ-ДПИТ-01).**

3. ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

3.1. Товарищество – ТОО «ТЭК-КАЗАХСТАН» (ТЭК), ТОО «ТД «ТЭК-КАЗАХСТАН» (ТД ТЭК).

3.2. **Руководство Товарищества –** Генеральный директор ТЭК/директор ТД ТЭК, либо лица их заменяющие

4. МЕТОДИКА

4.1 Политика в управлении информационной безопасностью направлена на достижение следующих целей:

4.1.1 обеспечение непрерывности основных бизнес-процессов;

4.1.2 минимизации возможных потерь и ущерба от нарушений в области информационной безопасности.

4.2 Для достижения указанных целей в Товариществе внедрены средства управления

информационной безопасности (далее – СУИБ), то есть соответствующие инструкции, положения, и процедуры которые соответствуют:

4.2.1 стандарту СТ РК ГОСТ Р ИСО/МЭК 15408;

4.2.2 требованиям законодательства Республики Казахстан, нормативным и договорным обязательствам Товарищества с точки зрения информационной безопасности;

4.2.3 действующей в Товарищества Политике по противодействию коррупции и мошенничеству **(Г-П-ДЭБ-01);**

4.2.4 правилам управления рисками Товарищества **(Г-РИ-Корп-01).**

4.3 СУИБ Товарищества документирована в настоящей Политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников Товарищества в области действия системы. Документированные требования СУИБ доводятся до сведения работников Товарищества.

4.4 Все информационные активы Товарищества, включая аппаратное обеспечение, программное обеспечение, информационные ресурсы на бумажных и электронных носителях, персонал, подлежат учету и категорированию в соответствии с их важностью и степенью доступа в соответствии с действующим в Товариществе Положением о конфиденциальной информации **(П-ЮД-03)/(П-03),** а также инструкцией Доступ к ресурсам автоматизированной системы **(Г-РИ-ДПИТ-01).**

4.5 В соответствии с установленными процедурами в области управления СУИБ, осуществляется регулярная оценка рисков информационной безопасности. При ее проведении учитывается вероятность угроз информационной безопасности и степень их влияния на бизнес-процессы, финансовое состояние и деловую репутацию Товарищества.

4.6 По результатам оценки рисков информационной безопасности выбираются и применяются средства управления для защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ.

4.7 Для обеспечения физической защиты информационных активов Товарищества, в границах области действия СУИБ (место расположения офиса ГО Товарищества) устанавливаются зоны безопасности и принимаются меры для предотвращения неавторизованного доступа в рабочие зоны и серверные помещения в соответствии с действующим в Товариществе Порядком доступа в серверные помещении **(РИ-ДПИТ-04).**

4.8 Товарищество стремится выявлять, учитывать и реагировать на инциденты в сфере информационной безопасности в соответствии с установленными процедурами.

4.9 В Товариществе будут установлены процедуры обеспечения непрерывности критических бизнес-процессов от эффектов существенных сбоев информационных систем или чрезвычайных ситуаций, контроля работоспособности СУИБ.

4.10 Работники Товарищества получают доступ к той информации, которая требуется для исполнения их функциональных обязанностей.

4.11 Товарищество проводит информирование, обучение и повышение квалификации работников в сфере информационных технологий.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1 Руководство Товарищества заявляет своё одобрение настоящей Политики, которая объявлена, распространена, внедрена и поддерживается на всех уровнях Товарищества.

5.2 Политика информационной безопасности Товарищества является общедоступным документом, который может предоставляться всем заинтересованным сторонам и размещается на официальном веб-сайте Товарищества.

5.3 Работники Товарищества несут ответственность за соблюдение требований документов СУИБ и правильную эксплуатацию технических и программных средств системы.

5.4 В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной документации и конфиденциальность информации, ставшей известной в силу выполнения своих обязанностей.

6. Приложения. Нет