	И-23 Политика информационной безопасности	Издание №2. Дата ввода: 15.03.2021г.	Стр. 1 из 6
		Взамен Издания №1 от 10.02.2020 г.	

УТВЕРЖДЕНО
решением Совета директоров
АО «КСЖ «Сентрас Коммеск Life»
протокол №08 от «15» марта 2021г.

И-23

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «КСЖ «СЕНТРАС КОММЕСК LIFE»

centras kommesk	И-23 Политика информационной безопасности	Издание №2. Дата ввода: 15.03.2021г.	Стр. 2 из 6
		Взамен Издания №1 от 10.02.2020 г.	

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ И ОБЛАСТЬ ПРИМЕНЕНИЯ	2
2. ЦЕЛИ, ЗАДАЧИ И ОСНОВНЫЕ ПРИНЦИПЫ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	2
3. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ДОСТУПА К СОЗДАВАЕМОЙ, ХРАНИМОЙ И ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ, МОНИТОРИНГА ИНФОРМАЦИИ И ДОСТУПА К НЕЙ.	3
4. ТРЕБОВАНИЯ К СБОРУ, КОНСОЛИДАЦИИ, ХРАНЕНИЮ И АНАЛИЗУ ИНФОРМАЦИИ ОБ ИНЦИДЕНТАХ ИБ	4
5. МОНИТОРИНГ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИБ	4
6. ИНФОРМАЦИОННЫЕ СИСТЕМЫ	4
7. МЕРЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	4
8. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ КОМПАНИИ.....	5
9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.....	6

1. ОБЩИЕ ПОЛОЖЕНИЯ И ОБЛАСТЬ ПРИМЕНЕНИЯ

- 1.1. Настоящая Политика информационной безопасности АО «КСЖ «Сентрас Коммекс Life» (далее – Политика) разработана в соответствии с законодательством Республики Казахстан, Требованиями к организации безопасной работы, обеспечивающей сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в страховой (перестраховочной) организации, а также кибербезопасности страховой (перестраховочной) организации, утвержденными постановлением Правления Национального Банка Республики Казахстан от 30 июля 2018 года №164 и Требованиями к деятельности организации по формированию и ведению базы данных, утвержденных постановлением Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 25 июня 2007 года №177.
- 1.2. Политика определяет систему взглядов на проблему обеспечения безопасности информации, содержит основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих внутренних документов АО «КСЖ «Сентрас Коммекс Life» (далее – Компания).
- 1.3. Положения Политики обязательны для исполнения всеми работниками Компании, стажерами, практикантами, исполнителями по заключенным Компанией договорам на оказание услуг, связанных со страховой деятельностью (далее – работники). Положения Политики должны доводиться до сведения клиентов и иных третьих лиц, имеющих доступ к информационным системам и документам Компании, в той их части, которая непосредственно взаимосвязана с Компанией и их деятельностью.
- 1.4. Действие Политики распространяется на все информационные системы и документы, владельцем и пользователем которых является Компания. Обеспечение информационной безопасности – необходимое условие для успешного осуществления деятельности Компании.
- 1.5. Под информационной безопасностью Компании (далее – ИБ) в настоящей Политике понимается состояние защищенности электронных информационных ресурсов, информационных систем и информационной инфраструктуры от внешних и внутренних угроз, которые могут привести к материальному ущербу, нанести ущерб репутации Компании или повлечь нанесение иного ущерба Компании, ее акционерам, работникам или клиентам.

2. ЦЕЛИ, ЗАДАЧИ И ОСНОВНЫЕ ПРИНЦИПЫ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

- 2.1. Система управления информационной безопасностью (далее – СУИБ) представляет собой часть общей системы управления Компании, которая предназначена для проектирования, реализации, контроля и совершенствования мер в области ИБ.
- 2.2. Целями СУИБ являются:
 - 1) обеспечение доступности, целостности и конфиденциальности информационных ресурсов Компании;
 - 2) минимизация уровня рисков, связанных с ИБ.
- 2.3. Задачами СУИБ являются:
 - 1) идентификация объектов защиты и выявление угроз;

centras kommesk	И-23 Политика информационной безопасности	Издание №2. Дата ввода: 15.03.2021г.	Стр. 3 из 6
		Взамен Издания №1 от 10.02.2020 г.	

- 2) разработка и реализация мероприятий по защите информационных ресурсов Компании;
 - 3) выявление, обработка и предотвращение инцидентов ИБ;
 - 3) оценка рисков ИБ;
 - 4) обучение и повышение уровня информированности работников Компании в области ИБ.
- 2.4. Построение СУИБ Компании и ее функционирование должны осуществляться в соответствии со следующими основными принципами:
- 1) законность – любые действия, предпринимаемые для обеспечения ИБ, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты;
 - 2) ориентированность на бизнес – ИБ рассматривается как процесс поддержки основной деятельности Компании. Любые меры по обеспечению ИБ не должны повлечь за собой серьезных препятствий деятельности Компании;
 - 3) непрерывность – построение и функционирование СУИБ осуществляется по фазам непрерывно повторяющегося цикла «Планирование – Реализация – Проверка – Корректировка»;
 - 4) комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;
 - 5) обоснованность и экономическая целесообразность – используемые средства защиты должны быть обоснованы с точки зрения заданного уровня безопасности и соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем ИБ должна быть меньше размера возможного ущерба от любых видов риска;
 - 6) приоритетность – при выборе методов и средств защиты оценивается степень важности информационных ресурсов Компании, а также потенциальных угроз ИБ;
 - 7) информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях ИБ и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер ИБ;
 - 8) взаимодействие и координация – меры ИБ осуществляются на основе взаимосвязи соответствующих структурных подразделений Компании, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами.

3. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ДОСТУПА К СОЗДАВАЕМОЙ, ХРАНИМОЙ И ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ, МОНИТОРИНГА ИНФОРМАЦИИ И ДОСТУПА К НЕЙ

- 3.1. Доступ к информации, хранимой и обрабатываемой в информационных системах Компании ограничивается в соответствии с внутренним документом И-58 «Положение о защите конфиденциальной информации в АО «КСЖ «Сентрас Коммекс Life» и предоставляется только тем работникам Компании, которым доступ необходим для выполнения служебных обязанностей.
- 3.2. Доступ к информации, хранимой и обрабатываемой в информационных системах Компании предоставляется только после идентификации и аутентификации работника.
- 3.3. Информация, хранимая и обрабатываемая в информационных системах Компании, регулярно оценивается на предмет необходимости ограничения доступа к ней в соответствии с внутренним документом И-58 «Положение о защите конфиденциальной информации в АО «КСЖ «Сентрас Коммекс Life»».
- 3.4. Информация, хранимая и обрабатываемая в информационных системах Компании, регулярно проверяется на предмет того, имеются ли признаки ее противоправного изменения либо удаления.
- 3.5. Служба информационной безопасности проводит регулярные проверки соответствия прав доступа, необходимых для выполнения служебных обязанностей фактическим правам доступа в информационных системах Компании.
- 3.6. Служба информационной безопасности осуществляет регулярный мониторинг как доступа к информации Компании, так и операций с ней.

centras kommesk	И-23 Политика информационной безопасности	Издание №2. Дата ввода: 15.03.2021г.	Стр. 4 из 6
		Взамен Издания №1 от 10.02.2020 г.	

4. ТРЕБОВАНИЯ К СБОРУ, КОНСОЛИДАЦИИ, ХРАНЕНИЮ И АНАЛИЗУ ИНФОРМАЦИИ ОБ ИНЦИДЕНТАХ ИБ

- 4.1. Служба информационной безопасности осуществляет сбор, консолидацию, хранение и анализ инцидентов ИБ в соответствии с внутренним документом, регулирующим мониторинг событий и обработку инцидентов информационной безопасности Компании.
- 4.2. Решение о проведении расследования инцидента информационной безопасности либо об отсутствии необходимости проведения такого расследования принимается Председателем Правления Компании на основании информации, предоставленной Службой информационной безопасности.
- 4.3. При этом Председатель Правления определяет необходимость привлечения к расследованию других подразделений Компании либо сторонних лиц, обладающих необходимыми знаниями и навыками.

5. КОНТРОЛЬ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИБ


- 5.1. Совет директоров Компании осуществляет мониторинг деятельности по обеспечению информационной безопасности на основании проверок внутреннего аудита, проводимых в соответствии с внутренним документом, регулирующим правила проведения внутреннего аудита в Компании.
- 5.2. При необходимости, Правление Компании инициирует проведение внешнего аудита деятельности по обеспечению информационной безопасности.

6. ИНФОРМАЦИОННЫЕ СИСТЕМЫ

- 6.1. К информационным системам Компании относятся:
 - 1) корпоративная информационно-аналитическая система КИАС:Страхование;
 - 2) система бухгалтерского учета 1С;
 - 3) почтовая система;
 - 4) контроллеры домена;
 - 5) файловые сервера;
 - 6) программно-технические средства защиты.

7. МЕРЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 7.1. Основными мерами по обеспечению ИБ Компании являются:
 - 1) административно-правовые и организационные меры;
 - 2) меры физической безопасности;
 - 3) программно-технические меры.
- 7.2. Административно-правовые и организационные меры включая:
 - 1) контроль за исполнением требований законодательства Республики Казахстан и внутренних документов;
 - 2) разработка, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;
 - 3) контроль соответствия бизнес-процессов требованиям Политики;
 - 4) информирование и обучение работников Компании работе с информационными системами и требованиям ИБ;
 - 5) реагирование на инциденты, локализацию и минимизацию последствий;
 - 6) анализ новых рисков ИБ;
 - 7) определение действий при возникновении чрезвычайных ситуаций;
 - 8) проведение профилактических мер при приеме на работу (заключении договоров) и увольнении (расторжении договоров) работников Компании.
- 7.3. Меры физической безопасности включая:
 - 1) организация пропускного и внутри объектового режимов;
 - 2) организация круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;
 - 3) организация противопожарной безопасности охраняемых объектов;
 - 4) контроль за доступом работников Компании в помещения ограниченного доступа.
- 7.4. Программно-технические меры включая:
 - 1) использование лицензионного программного обеспечения и сертифицированных средств защиты информации;

	И-23 Политика информационной безопасности	Издание №2. Дата ввода: 15.03.2021г.	Стр. 5 из 6
		Взамен Издания №1 от 10.02.2020 г.	

- 2) использование средств защиты периметра (firewall, прокси-сервера и т.п.);
- 3) применение комплексной антивирусной защиты;
- 4) использование средств ИБ, встроенных в информационные системы;
- 5) использование специальных комплексов ИБ;
- 6) обеспечение регулярного резервного копирования информации;
- 7) контроль за правами и действиями пользователей, в первую очередь, за действиями пользователей привилегированных учетных записей;
- 8) применение систем криптографической защиты информации;
- 9) обеспечение безотказной работы аппаратных средств;
- 10) мониторинг состояния критичных элементов информационной системы.

8. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ КОМПАНИИ ЗА ОБЕСПЕЧЕНИЕ ИБ ПРИ ИСПОЛНЕНИИ ФУНКЦИОНАЛЬНЫХ ОБЯЗАННОСТЕЙ

- 8.1. Правление Компании:
 - 1) осуществляет стратегическое планирование;
 - 2) утверждает внутренние нормативные документы;
 - 3) определяет полномочия и ответственность подразделений в области ИБ;
 - 4) координирует деятельность всех подразделений для организации и поддержания соответствующего уровня ИБ;
 - 5) выделяет достаточные ресурсы для разработки, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования системы ИБ;
 - 6) принимает решения о критериях принятия рисков и допустимом уровне риска;
 - 7) обеспечивает проведение внешних и внутренних проверок состояния ИБ;
 - 8) проводит ежегодный анализ состояния ИБ;
 - 9) отвечает за общее состояние ИБ.
- 8.2. Совет директоров утверждает политику ИБ, перечень защищаемой информации, включающий, в том числе информацию о сведениях, составляющих тайну страхования, служебную, коммерческую или иную охраняемую законом тайну, и порядок работы с защищаемой информацией.
- 8.3. Совет директоров осуществляет контроль за состоянием СУИБ, в том числе с помощью плановых и внеплановых проверок проводимых СВА.
- 8.4. Правление утверждает внутренние документы Компании, регламентирующие процесс обеспечения ИБ, а также порядок и периодичность их пересмотра.
- 8.5. Служба информационной безопасности:
 - 1) организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности подразделений Компании по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;
 - 2) разрабатывает политику информационной безопасности Компании;
 - 3) обеспечивает методологическую поддержку процесса обеспечения информационной безопасности Компании;
 - 4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности Компании в рамках своих полномочий;
 - 5) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;
 - 6) осуществляет анализ информации об инцидентах информационной безопасности;
 - 7) организует и проводит мероприятия по обеспечению осведомленности работников Компании в вопросах информационной безопасности;
 - 8) осуществляет мониторинг состояния системы управления информационной безопасностью Компании;
 - 9) осуществляет информирование руководства Компании о состоянии системы управления информационной безопасностью.
- 8.6. Служба хозяйственного управления и безопасности:
 - 1) реализует меры физической и технической безопасности в Компании, в том числе организует пропускной и внутриобъектовый режим;
 - 2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз ИБ путем предоставления минимально необходимого для выполнения должностных обязанностей физического доступа при приеме на работу, своевременного изъятия

centras kommesk	И-23 Политика информационной безопасности	Издание №2. Дата ввода: 15.03.2021г.	Стр. 6 из 6
		Взамен Издания №1 от 10.02.2020 г.	

выданных документов архива и ограничения физического доступа в помещения Компании при увольнении.

8.7. HR Служба:

1) обеспечивает подписание работниками Компании, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;

2) участвует в организации процесса повышения осведомленности работников Компании в области ИБ.

8.8. Юридический департамент осуществляет правовую экспертизу внутренних документов Компании по вопросам обеспечения ИБ.

8.9. Комплаенс-контролер совместно с юридическим департаментом определяет виды информации, подлежащие включению в перечень защищаемой информации.

8.10. Служба внутреннего аудита проводит оценку состояния СУИБ в соответствии с внутренними документами, регламентирующими организацию системы внутреннего аудита Компании.

8.11. Департамент информационных технологий:

1) разрабатывает схемы информационной инфраструктуры Компании;

2) обеспечивает предоставление доступа работникам к информационным активам Компании;

3) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности информационных систем Компании (включая резервирование и (или) архивирование) в соответствии с внутренними документами страховой (перестраховочной) организации;

4) обеспечивает соблюдение внутренних документов Компании, содержащих требования к информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем Компании.

8.12. Каждый работник Компании несет ответственность за соблюдение утвержденных документов по обеспечению ИБ, своевременное извещение своих руководителей и Службы информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

8.13. Руководители подразделений Компании несут ответственность за ознакомление работников с требованиями ИБ и обеспечение ИБ в возглавляемых ими подразделениях.

8.14. Все намеренные либо ненамеренные действия или бездействия работников Компании, связанные с нарушением требований ИБ, могут рассматриваться Правлением Компании как основание для наложения мер дисциплинарного взыскания.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящая Политика вводится в действие с момента ее утверждения Советом директоров Компании.

9.2. В настоящую Политику могут быть внесены изменения и (или) дополнения путем утверждения документа в новой редакции.

9.3. Настоящая Политика пересматривается и при необходимости актуализируется не реже одного раза в год.

9.4. Если в результате изменения законодательства Республики Казахстан или требований уполномоченного органа отдельные пункты настоящей Политики вступают в противоречие с ними, то эти положения утрачивают силу, и, до момента внесения изменений в настоящую Политику, Компания руководствуется действующими на соответствующий момент времени положениями законодательства Республики Казахстан и/или требованиями уполномоченного органа.