Утверждено решением
Директора
ТОО «Страховой Брокер «Tumar»
от «08» апреля 2024 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТОО «СТРАХОВОЙ БРОКЕР «TUMAR»

г. Алматы, 2024 г.

1. Общие положения и область применения

1. ТОО «Страховой Брокер» «Tumar» (далее — Общество), осуществляющее деятельность в отрасли «общее страхование», в пределах соответствующих классов страхования, с учетом особенностей совмещения отраслей и классов страхования, установленных Законом Республики Казахстан «О страховой деятельности». Деятельность Общества заключается в предоставлении услуг страхования и связана с обработкой и хранением информации, являющейся важным информационным активом, и требует обеспечения информационной безопасности, под которой понимается процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов Общества.
2. Настоящая Политика информационной безопасности (далее — Политика) является внутренним нормативным документом Общества, которая определяет единый подход в обеспечении информационной безопасности в Обществе, направленного на организацию защиты информационных активов вне зависимости от формы и места ее обработки и хранения, средств ее обработки.
3. Нормативно-правовую основу Политики составляет законодательство Республики Казахстан по вопросам использования информационных систем, Требования 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, утвержденные постановлением Правления Национального Банка Республики Казахстан от 30 июля 2018 года N2 164 (далее — Постановление НБ РК N2164), требования стандарта СТ РК ISO/IEC 27001 (Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования и иные нормативные правовые акты Республики Казахстан).
4. Общество организует безопасную работу, обеспечивающую сохранность и защиту информации от несанкционированного доступа к данным, хранящимся в Обществе, а также кибербезопасность Общества, путем создания, мониторинга и усовершенствования системы управления информационной безопасностью (далее — СУИБ), являющейся частью общей системы управления Обществом, предназначенной для управления процессом обеспечения информационной безопасности.
5. Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информации и/или поддерживающей инфраструктуры. Политика охватывает все информационные системы Общества, технологические платформы, аппаратно-программные комплексы, сети телекоммуникаций, а также системы обеспечения бесперебойного функционирования технических средств и информационной безопасности, собственником, владельцем и пользователем которых является Общество.

6. Ответственным за информационную безопасность является специалист ИБ, который напрямую подчиняется высшему руководству Общества.
7. Положения Политики обязательны к исполнению всеми работниками Общества и доводится до сведения вновь принятых работников, практикантов, стажеров, клиентов и иных третьих лиц, имеющих доступ к информационным активам Общества.

2. Управление информационными ресурсами

8. Общество разрабатывает, документирует и использует критерии классификации информационных ресурсов для бизнеса.
9. Общество ведет учет всех информационных ресурсов и назначает владельцев для каждого информационного ресурса.
10. Общество определяет, документирует и использует правила приемлемого использования информационных ресурсов, а также технологий и средств их обработки, включая следующий перечень, но не ограничиваясь им: сеть Интернет, электронная почта, носители информации.
11. Общество устанавливает ответственность владельцев за управление информационными ресурсами Общества, а также за определение и реализацию в отношении информационных ресурсов необходимых защитных мер.

3. Цели, задачи и основные принципы построения СУИБ

12. Главной целью СУИБ Общества является снижение вероятности нанесения материального, репутационного или иного ущерба Обществу, её партнерам, клиентам и работникам в результате реализации угроз ИБ.
13. Указанная цель достигается посредством управления рисками информационной безопасности при решении задач по обеспечению и постоянному поддержанию следующего состояния информационных ресурсов и информационных систем:

- обеспечение высокой доступности и целостности всех внутренних и внешних (предоставляемым клиентам и партнерам) информационных систем Общества;
- обеспечение конфиденциальности, целостности и доступности всей критичной информации Общества;
- обеспечение необходимой защиты данных контрагентов Общества и информации работников Общества (в том числе персональных данных);
- отнесение информации к категории несекретной, ограниченного распространения, страховой, коммерческой и другим видам тайн, иной конфиденциальной информации, подлежащей защите от неправомерного использования;
- обеспечение и управление корпоративной безопасностью;

- защита от вмешательства в процесс функционирования информационных систем;
- разграничение прав доступа к информации, аппаратно-программным средствам, средствам защиты, объектам и помещениям, размещающим информационные ресурсы;
- регистрация происходящих событий ИБ в информационной среде;
- прогнозирование и своевременное выявление угроз безопасности информационными активам Общества, причин и условий, способствующих нанесению финансового, материального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования Общества с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Общества, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц;
- гарантирование достаточности мер и непрерывности защиты информационных активов Общества от угроз информационной безопасности;
- поддержание структурированной и всесторонней системы идентификации и оценки рисков информационной безопасности, выбора и применения соответствующих средств защиты, управления, измерения и улучшения их эффективности;
- соответствие требованиям законодательства Республики Казахстан;
- повышение культуры информационной безопасности работников Общества.
- Общество защищает важные записи от утраты, разрушения и фальсификации.
- специалист ИБ Общества поддерживает контакты с полномочными органами, профессиональными сообществами, профессиональными ассоциациями или форумами специалистов по информационной безопасности.
- На ежегодной основе специалист ИБ проходит обучение (курсы) по информационной безопасности, а также доводит актуальные рекомендации в сфере ИБ до всех сотрудников Общества путем

рассылок на корпоративную почту, общий чат либо другим доступным способом и проведением семинаров.

- Руководство Общества утверждает следующие меры для обеспечения безопасности передаваемой информации - в случае необходимости передачи информации сотрудники Общества, должны проявлять бдительность и осторожность в процессе передачи информации; любая информации должна передаваться только авторизованным лицам с использованием доверенных средств передачи.

4. Управление персоналом

14. Общество устанавливает ответственность работников, контрагентов и третьих сторон по обеспечению ИБ информационных ресурсов Общества.
15. Общество регламентирует, документирует и использует процедуры проверки кандидатов на вакантные должности, контрагентов и третьих сторон.
16. Общество предоставляет и формально фиксирует доступ к информационным ресурсам Общества только после заключения между Обществом и кандидатом на вакантную должность/контрагентом/третьей стороной соглашения о неразглашении конфиденциальной информации Общества и ознакомления кандидата на вакантную должность/контрагента/третьей стороны с обязанностями по соблюдению требований ИБ.
17. Общество регламентирует, документирует и проводит мероприятия с целью повышения осведомленности работников/контрагентов/третьих сторон в вопросах обеспечения безопасности информационных ресурсов Общества.
18. Общество устанавливает и фиксирует персональную ответственность за нарушение или неисполнение требований по обеспечению ИБ информационных ресурсов Общества.
19. Общество регламентирует, документирует и использует процедуры увольнения, прекращения трудовых и договорных отношений.
20. Увольнение или прекращение трудовых и договорных отношений сопровождаются возвратом работниками/контрагентами/третьими сторонами информационных ресурсов Общества и прекращением доступа работников/контрагентов/третьих сторон к информационным ресурсам Общества.
21. Руководители подразделений Общества:
    1) обеспечивают ознакомление работников с требованиями к информационной безопасности;
    2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях.
22. Работники подразделений Общества:

1) обеспечивают соблюдение требований к информационной безопасности, принятых в Обществе;

2) к сотрудникам, совершившим нарушение требований безопасности, применяется дисциплинарная практика, установленная в организации в соответствии с законодательством РК;

3) извещают своего непосредственного руководителя и подразделение по информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

5. Заключительные положения

23. Настоящая Политика подлежит пересмотру в случае существенных изменений в деятельности Общества, изменения законодательства Республики Казахстан или регулирующих органов, изменений международных стандартов в сфере информационной безопасности, влияющих на СУИБ, а также пересматривается с целью анализа и актуализации изложенной в них информации не реже одного раза в два года.

24. Настоящая Политика вступает в действие со дня её утверждения.

Изменения и дополнения, внесенные решением Генерального Директора (дата/№):

№	Внесены изменения, дополнения	Дата		Рег.У2

Признано утратившим силу решением Генерального Директора Общества (протокол №____)