Annex No. 1 to the Minutes No. 24/2024 of the Board of Directors Meeting
Приложение № 1 к Протоколу № 24/2024 Заседания Совета Директоров

УТВЕРЖДЕНО:
Решением Совета Директоров
АО «Европейская Страховая Компания»
Протокол № 24/2024 от «12» августа 2024г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Акционерного общества
Компании по Страхованию Жизни
«Европейская Страховая Компания»

г. Алматы 2024г.

EUROPEAN INSURANCE COMPANY

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ 3

2. ЦЕЛЬ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ 3

2.1 Цель обеспечения информационной безопасности Компании: 3
2.2 Основные задачи системы информационной безопасности Компании: 3

3. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ДОСТУПА К СОЗДАВАЕМОЙ, ХРАНИМОЙ И ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ КОМПАНИИ, МОНИТОРИНГА ИНФОРМАЦИИ И ДОСТУПА К НЕЙ..... 4

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

5. РАЗДЕЛЕНИЕ ПОЛНОМОЧИЙ И ОТВЕТСТВЕННОСТЬ 5

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ 5

1. Общие положения

Настоящая Политика информационной безопасности (далее - Политика) Акционерного общества Компании по Страхованию Жизни «Европейская Страховая Компания» (далее – Компания) определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности в Компании, служит руководством при разработке соответствующих внутренних положений, правил, инструкций Компании.

Нормативно-правовую основу настоящей Политики составляет действующее законодательство Республики Казахстан по вопросам использования информационных систем и обеспечения информационной безопасности, нормативные правовые акты Республики Казахстан, требования международного стандарта по информационной безопасности ISO/IEC 27001:2013.

Обеспечение информационной безопасности – это необходимое условие для успешного осуществления коммерческой деятельности Компании. Компания рассматривает информацию как один из важнейших активов. Информационная безопасность является составной частью общей политики Компании в сфере обеспечения безопасности бизнеса. Нарушения в данной области могут привести к серьезным последствиям, в том числе к потере доверия со стороны клиентов и снижению конкурентоспособности.

Неотъемлемой частью организации защиты информации является непрерывный контроль эффективности предпринимаемых мер, определение для работников Компании перечня недопустимых действий, возможных последствий и ответственности.

Реализация настоящей Политики исходит из предпосылки, что невозможно обеспечить требуемый уровень защищённости информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы рассматриваются как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

Термины и определения, используемые в настоящей Политике, применяются в соответствии со значением, регламентированным соответствующими нормативными – правовыми актами Республики Казахстан и положениями международного стандарта по информационной безопасности.

2. Цель и задачи защиты информационной системы

2.1 Цель обеспечения информационной безопасности Компании:

Целью системы информационной безопасности является защита информационных систем Компании для снижения угроз информационной безопасности и минимизации уровня рисков.

2.2 Основные задачи системы информационной безопасности Компании:

2.2.1.1 Своевременное выявление потенциальных угроз безопасности и уязвимостей объектов защиты.

2.2.2 Предотвращение инцидентов информационной безопасности.

2.2.2.1 Создание условий функционирования Компании с наименьшей вероятностью реализации угроз безопасности информационных ресурсов.

2.2.2.2 Создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании информационных систем Компании на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности.

3. Требования к организации доступа к создаваемой, хранимой и обрабатываемой информации в информационных системах Компании, мониторинга информации и доступа к ней

3.1 Доступ к информации, хранимой и обрабатываемой в информационных системах Компании, ограничивается в соответствии с внутренними документами Компании и предоставляется только тем сотрудникам структурных подразделений Компании, которым доступ необходим для выполнения служебных обязанностей.

3.2 Доступ к информации, хранимой и обрабатываемой в информационных системах Компании, предоставляется только после соответствующей идентификации и аутентификации работника.

3.3 Информация, хранимая и обрабатываемая в информационных системах Компании, регулярно проверяется на предмет необходимости ограничения доступа к ней в соответствии с внутренним документом Компании, регламентирующим работу с конфиденциальной информацией в Компании.

3.4 Информация, хранимая и обрабатываемая в информационных системах Компании, регулярно проверяется на предмет того, имеются ли признаки ее противоправного изменения, копирования либо удаления.

3.5 Ответственный сотрудник Компании за обеспечение информационной безопасности проводит проверки соответствия прав доступа, необходимых для выполнения служебных обязанностей фактическим правам доступа в информационных системах Компании.

3.6 Ответственный сотрудник Компании за обеспечение информационной безопасности осуществляет регулярный мониторинг как доступа к информации Компании, так и операций с ней.

4. Требования к сбору, консолидации, хранению и анализу информации об инцидентах информационной безопасности

4.1 Ответственное подразделение/сотрудник Компании за обеспечение информационной безопасности осуществляет сбор, консолидацию, хранение и анализ инцидентов информационной безопасности в соответствии с внутренним документом, регулирующим мониторинг событий и обработку инцидентов информационной безопасности Компании.

4.2 В случае необходимости принимаются соответствующие меры по устранению инцидента информационной безопасности, как только стало известно о возникновении инцидента. Непосредственно после устранения инцидента принимаются надлежащие меры по выявлению и устранению причин и последствий инцидента.

4.3 При необходимости, после устранения инцидента информационной безопасности осуществляется информирование курирующего члена Правления и (или) Правление Компании, включая информирование о причинах и последствиях инцидента (после получения результатов обработки инцидента).

4.4 По результатам обработки инцидента информационной осуществляется анализ причин возникновения инцидента информационной безопасности, его механизма и последствий. По результатам анализа инцидента информационной безопасности готовится заключение, в котором отражается вся информация об инциденте информационной безопасности, а также предложения по принятию корректирующих мер в целях снижения вероятности и возможного ущерба от повторного инцидента информационной безопасности.

4.5 Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению не менее 5 (пяти) лет с момента осуществления анализа и принятия соответствующих мер по недопущению подобного инцидента информационной безопасности в будущем.

5. Разделение полномочий и ответственность

5.1 Руководители структурных подразделений Компании:

1) обеспечивают ознакомление сотрудников структурных подразделений Компании с требованиями к информационной безопасности в Компании;

2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях.

5.2 Сотрудники структурных подразделений Компании:

1) несут ответственность за соблюдение требований настоящей Политики, а также иных внутренних нормативных документов Компании по обеспечению информационной безопасности в Компании;

2) контролируют исполнение требований информационной безопасности, регламентированных в настоящей Политике и других внутренних нормативных документах Компании, третьими лицами, с которыми они контактируют в рамках своих должностных обязанностей, в том числе путем включения указанных требований в договоры с третьими лицами;

3) обязаны извещать своего непосредственного руководителя и ответственное подразделение/сотрудника Компании за обеспечение информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными ресурсами.

5.3 Все намеренные либо ненамеренные действия или бездействия сотрудников структурных подразделений Компании, связанные с нарушением требований информационной безопасности, могут рассматриваться Правлением Компании как основание для наложения мер дисциплинарного взыскания.

6. Заключительные положения

6.1 Настоящая Политика вступает в силу с момента ее утверждения Советом директоров Компании. При этом, утрачивает силу Политика Информационной безопасности Акционерного общества Компании по Страхованию Жизни «Европейская Страховая Компания», утвержденная решением Совета Директоров Компании в Протоколе №22/2021 от 08 октября 2021г.

6.2 Пересмотр положений настоящей Политики осуществляется на регулярной основе, но не реже одного раза в три года. Внеплановый пересмотр настоящей Политики должен осуществляться в случае:

1) изменения нормативно – правовых актов Республики Казахстан, внутренних документов Компании, определяющих требования информационной безопасности;
2) выявления снижения общего уровня информационной безопасности Компании (по результатам внутреннего или внешнего аудита);
3) существенных изменений организационной и/или технологической инфраструктуры, ресурсов и бизнес-процессов Компании;
4) выявления существенных недостатков при выполнении мероприятий, регламентированных настоящей Политикой, а также противоречий ее положений с другими внутренними документами Компании.
Пересмотр настоящей Политики, а также внесение в нее изменений выполняется в соответствии с порядком, установленным в Компании.

6.3 В случае если отдельные нормы настоящей Политики вступят в противоречие с действующим законодательством Республики Казахстан и/или Уставом Компании, они утрачивают силу и в дальнейшем применяются соответствующие нормы законодательства Республики Казахстан и/или Устава Компании. Недействительность отдельных норм настоящей Политики не влечет недействительность других норм и Политики в целом.