Приложение №1

к приказу № 05-А от 10.03.2025 г.

УТВЕРЖДЕНО

приказом ООО Страховая компания «АСТК»
от 10.03.2025 г. № 05-А

Положение о защите конфиденциальной информации в ООО Страховая компания «АСТК»

Версия 1.0

Москва, 2025

Содержание

История изменений

Версия	Описание изменений	Автор	Дата
1.0	Разработка документа	Солянкин Е.С.	10.03.2025

1. Общие положения

1.1. Положение о защите конфиденциальной информации в ООО Страховая компания «АСТК» (далее – Положение) определяет общий порядок обеспечения защиты конфиденциальной информации в ООО Страховая компания «АСТК» (далее - Компания), перечень сведений, составляющих конфиденциальную информацию.

1.2. Целью настоящего Положения является определение надлежащих правил обращения с конфиденциальной информацией для предотвращения ее утечки, хищения, утраты или искажения. Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации, а также внутренними нормативными документами Компании, в том числе:

– Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ 149);

– Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (далее – ФЗ 98);

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ 152);

– Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ 224);

– Постановление Правительства РФ от 19.07.2022 № 1299 «Об утверждении списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль»;

– Указ Президента Российской Федерации от 06.03. 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (далее – Указ № 188);

– Указ Президента РФ от 04.08.2004 № 1009 «Об утверждении Перечня стратегических предприятий и стратегических акционерных обществ»;

– Внутренний стандарт Всероссийского союза страховщиков «Обеспечение защиты конфиденциальной информации при осуществлении страховой деятельности».

1.3. Настоящим Положением устанавливается:

– порядок отнесения сведений к категории конфиденциальной информации;

– режим защиты конфиденциальной информации;

– обязанности работников Компании по защите конфиденциальной информации;

– порядок доступа к конфиденциальной информации;

– порядок работы с конфиденциальной информацией;

– порядок предоставления сторонним организациям сведений, составляющих конфиденциальную информацию;

– роли работников Компании по защите конфиденциальной информации;

– ответственность за разглашение конфиденциальной информации Компании, утрату документов, содержащих такую информацию и нарушение порядка работы с ними.

1.4. Для отдельной категории информации, по решению руководства Компании, может быть установлен особый порядок обращения с ней, регламентируемый специальными нормативными документами (положениями, инструкциями, правилами).

1.5. Требования настоящего Положения обязательны для исполнения всеми работниками Компании, которые несут персональную ответственность за сохранность и обеспечение защиты сведений, содержащих конфиденциальную информацию.

1.6. В настоящем Положении используются следующие основные понятия и условные обозначения.

АРМ – Автоматизированное рабочее место.

ИБ – Информационная безопасность.

Информационный актив – это материальный или нематериальный объект, который является информацией или содержит информацию, служит для обработки, хранения или передачи информации и имеет ценность для Компании.

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Конфиденциальность – свойство ИБ, состоящее в том, что обработка, хранение и передача информационных активов осуществляются таким образом, что информационные активы доступны только авторизованным Пользователям, объектам системы или процессам.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и требованиями Компании.

К конфиденциальной информации в Компании отнесены:

– информация, содержащая страховую тайну – полученные Компанией в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и/или выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц (состав этой информации, а также ее правовой режим определен в ст. 946 Гражданского кодекса Российской Федерации);

– информация, составляющая коммерческую тайну – сведения любого характера (технические, экономические, организационные и другие), а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

– персональные данные (любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в соответствии с ФЗ-152) работников Компании / бывших работников Компании / лиц, которые предоставили свои персональные данные для целей соискания должности в Компании, клиентов Компании / представителей клиентов Компании / потенциальных клиентов Компании и иных субъектов персональных данных, определенных в соответствии с внутренними нормативными документами Компании;

– инсайдерская информация в соответствии с ФЗ-224;

– конфиденциальная информация, полученная от ее обладателя (физического или юридического лица, индивидуального предпринимателя) законным способом (на основании договора или ином законном основании);

– иные сведения, предусмотренные Указом Президента РФ от 6 марта 1997 г. №188 или отнесенные к конфиденциальной информации в соответствии с настоящим Положением.

Общедоступная информация – информация, не являющаяся конфиденциальной, в том числе:

– сведения, содержащиеся в сообщениях и отчетах, официально опубликованных Компанией в соответствии с действующим законодательством Российской Федерации;

– сведения, содержащиеся в официальных пресс-релизах, а также рекламных сообщениях Компании;

– сведения, опубликованные в средствах массовой информации по инициативе третьих лиц и с разрешения руководства Компании;

– сведения, обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена законодательством Российской Федерации.

Пользователь – работник Компании, работающий по трудовому договору, а также специалисты, оказывающие услуги (выполняющие работы) для Компании на основании гражданско-правового договора, а также представители юридических лиц, имеющих с Компанией договорные отношения, (подрядчики, аудиторы и т.п.).

Руководство Компании – Генеральный директор.

2. Порядок отнесения сведений к категории конфиденциальной информации

2.1. Отнесение сведений к категории конфиденциальной информации осуществляется обладателем (владельцем) такой информации в порядке, установленном законодательством Российской Федерации, а также на основании Перечня сведений, составляющих конфиденциальную информацию (далее – Перечень сведений). Перечень сведений приведен в Приложении №1 к настоящему Положению.

2.2. Информация (документ) относится к конфиденциальной информации в том случае, если содержит или составляет сведения из Перечня сведений.

2.3. Информация, включаемая в Перечень сведений, должна отвечать следующим критериям:

− ее открытое использование связано с ущербом для Компании, в том числе потенциальным;

− она не является общеизвестной или общедоступной на законных основаниях;

− принятие мер по сохранению ее конфиденциальности обусловлено требованиями законодательства Российской Федерации, соображениями экономической и иной выгоды Компании;

− информация нуждается в защите, т.к. она не относится к категории государственных секретов, и не защищена авторским и патентным правом;

− ее сокрытие не наносит ущерба Компании и не несет правовых рисков в соответствии с действующим законодательством Российской Федерации.

2.4. Наличие конфиденциальной информации в документе (таблица, письмо, отчет, инструкция, положение, регламент и пр.) определяется исполнителем на основании Перечня сведений. В случае возникновения затруднений при определении конфиденциальности информации исполнителю необходимо обратиться к своему непосредственному руководителю и / или Руководителю направления информационной безопасности.

2.5. Дополнения и изменения к Перечню сведений вносятся на основе предложений работников структурных подразделений Компании с учетом действующего законодательства Российской Федерации, внутренних нормативных документов и интересов Компании.

2.6. Если информация не предусмотрена Перечнем сведений, а, по мнению работника, может являться конфиденциальной, работник предоставляет Руководителю направления информационной безопасности аргументированные предложения о необходимости защиты этой информации и внесении соответствующих дополнений в Перечень сведений. До принятия окончательного решения защита данной информации должна быть обеспечена в соответствии с требованиями настоящего Положения.

3.Доступ работников и сторонних лиц к конфиденциальной информации

3.1. При трудоустройстве в Компанию работники должны быть предупреждены об ответственности за разглашение конфиденциальной информации Компании. Факт ознакомления фиксируется путем подписания при трудоустройстве в Компанию работником обязательства о неразглашении конфиденциальной информации Компании. Форма обязательства о неразглашении конфиденциальной информации Компании приведена в Приложении №2 к настоящему Положению.

3.2. К конфиденциальной информации Компании имеют право доступа Пользователи, получившие доступ к конфиденциальной информации Компании в порядке, определенном настоящим Положением

и иными внутренними нормативными документами Компании.

3.3. Работники Компании должны иметь доступ к конфиденциальной информации только в пределах выполнения своих должностных обязанностей и к той конфиденциальной информации, которая необходима для выполнения должностных обязанностей, и только после подписания письменного обязательства о неразглашении конфиденциальной информации.

3.4. Документом, разрешающим допуск работника к конфиденциальной информации, является подписанное работником обязательство о неразглашении конфиденциальной информации Компании.

3.5. Доступ (предоставление, передача) к конфиденциальной информации третьих лиц может осуществляться на основании действующих договоров / соглашений, согласованных Директором по юридическим вопросам и заинтересованными подразделениями. Договоры должны в том числе предусматривать обязанности третьих лиц по защите конфиденциальной информации Компании, доступ к которой получен в рамках соглашения, а также меры защиты при ее обработке[1]. При отсутствии договора/соглашения решение о допуске (передаче) к конфиденциальной информации Компании сторонних лиц принимается по инициативе руководителя инициирующего подразделения по разрешению Руководства Компании[2].

3.6. Руководители структурных подразделений обязаны обеспечивать контроль за допуском подчиненных работников к конфиденциальной информации и принимать меры по обоснованному ограничению количества лиц, имеющих доступ к соответствующей информации. Руководители должны ограничивать объем запрашиваемых для подчиненных работников прав доступа исключительно правами, минимально необходимыми для выполнения должностных обязанностей.

3.7. Доступ к ресурсам локально-вычислительной сети Компании (в том числе, содержащим конфиденциальную информацию) предоставляется в соответствии с внутренними нормативными документами Компании.

3.8. Каждый Пользователь, имеющий доступ в локально-вычислительную сеть Компании, должен работать в ней и с ее ресурсами (в том числе, содержащими конфиденциальную информацию) в строгом соответствии с внутренними нормативными документами Компании.

3.9. Принятие на себя обязательства о неразглашении конфиденциальной информации осуществляется Пользователями на добровольной основе.

3.10. В случаях, если при заключении договоров с юридическими и физическими лицами на основании заключенных договоров (либо иных оснований) они должны иметь доступ к конфиденциальной информации Компании, между Компанией и этим лицом подписывается Соглашение о конфиденциальности. Приоритетно должны использоваться типовые формы Соглашений о конфиденциальности, утвержденные в Компании. Ответственность за своевременную подготовку данного Соглашения возлагается на руководителя структурного подразделения Компании - инициатора заключения договора (контракта) с данным лицом. Подписантом Соглашения о конфиденциальности должен выступать руководитель структурного подразделения Компании - инициатора заключения договора (контракта) или Генеральный директор. Соглашения о конфиденциальности, отличные от типовых форм Компании, должны согласовываться с Директором по юридическим вопросам и Руководителем направления информационной безопасности.

---

[1] В данном документе под обработкой конфиденциальной информации подразумевается операция или совокупность действий, совершаемых с использованием средств автоматизации или без их использования, в том числе передача, хранение, использование, уничтожение

[2] Раскрытие конфиденциальной информации третьим лицам в случае обоснованной бизнес-необходимости возможно без договора/соглашения и разрешения Руководства Компании, если объем раскрываемой информации незначителен и ее открытое использование в этом объеме не связано с ущербом для Компании

4. Режим конфиденциальности информации

4.1. Меры по охране конфиденциальности информации, принимаемые Компанией, включают в себя:

- определение Перечня сведений, составляющих конфиденциальную информацию Компании, и установление в отношении такой информации режима конфиденциальности;
- ограничение доступа к конфиденциальной информации путем установления порядка доступа к этой информации и контроля за его соблюдением;
- регулирование отношений по использованию конфиденциальной информации работниками на основании трудового договора и внутренних нормативных документов Компании;
- регулирование отношений по использованию (передаче) конфиденциальной информации сторонними лицами, в том числе на основании Соглашений о конфиденциальности или соответствующих пунктов договоров;

4.2. В случае установления в Компании режима коммерческой тайны наряду с мерами, указанными в п. 4.1 настоящего Положения, должны применяться следующие меры по охране коммерческой тайны:

- учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (полное наименование и место нахождения). Шаблон грифа «Коммерческая тайна» приведен в Приложении №3 к настоящему Положению.

4.3. Режим конфиденциальности информации считается установленным после принятия Компанией мер, указанных в пункте 4.1. настоящего Положения.

4.4. Наряду с мерами, указанными в п. 4.1 настоящего Положения, Компания вправе применять при необходимости средства и методы технической защиты информации, а также другие не противоречащие законодательству Российской Федерации меры.

4.5. Меры по установлению режима конфиденциальности информации признаются достаточными, если:

- исключен доступ к конфиденциальной информации любых лиц без согласия Компании;
- обеспечена возможность использования конфиденциальной информации работниками и передачи ее контрагентам без нарушения режима конфиденциальности информации.

4.6. Контроль, организация, разработка и реализация мер по защите конфиденциальной информации осуществляется Руководителем направления информационных технологий и Руководителем направления информационной безопасности.

4.7. Конфиденциальная информация не подлежит разглашению и передаче третьим лицам, не допущенным в установленном порядке к работе с этой информацией, за исключением случаев, предусмотренных действующим законодательством Российской Федерации

4.8. Допуск к конфиденциальной информации Компании работников других организаций и государственных структур осуществляется согласно пп.3.5, 3.7.

4.9. Обладателем конфиденциальной информации, полученной в рамках трудовых отношений и в результате трудовой деятельности работника, является Компания.

4.10. Конфиденциальная информация, полученная от ее обладателя на основании договора или ином законном основании, считается полученной законным способом и защищается аналогично конфиденциальной информации Компании.

4.11. Конфиденциальная информация, обладателем которой является Компания, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых Компанией мер по охране конфиденциальности этой информации, а также, если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация является конфиденциальной, обладателем ее является Компания и что осуществляющее передачу лицо не имеет на передачу информации законного основания.

5. Обязанности работников Компании по защите конфиденциальной информации

5.1. Работники Компании обязаны:

– знать и выполнять требования, предъявляемые при работе с конфиденциальной информацией и определенные в настоящем Положении и иных внутренних документах Компании;

– знать Перечень сведений;

– классифицировать обрабатываемую информацию на основании Перечня сведений;

– обеспечивать сохранность конфиденциальной информации, ставшей им известной в ходе выполнения должностных обязанностей;

– использовать только с ту информацию, которая необходима для выполнения должностных обязанностей и в соответствии с внутренними нормативными документами Компании; наличие технической возможности ознакомления с информацией не является гарантией того, что данная информация разрешена к ознакомлению (и дальнейшим манипуляциям) в рамках должностных обязанностей работника;

– организовать работу с конфиденциальной информацией на рабочем месте так, чтобы исключить возможность ознакомления с конфиденциальной информацией посторонних лиц, в том числе допущенных к подобным работам и документам, но не имеющим к ним прямого отношения;

– предпринимать разумные меры, предотвращающие несанкционированный доступ к конфиденциальным документам или хищение средств обработки и хранения конфиденциальной информации во время своего отсутствия на рабочем месте;

– по возможности пресекать действия работников и посторонних лиц, которые могут привести к разглашению конфиденциальной информации, незамедлительно информировать руководителя структурного подразделения (непосредственного руководителя) и Руководителя направления информационной безопасности (по электронной почте ibmon@astk-insur.ru) о таких действиях и о других фактах нарушения режима конфиденциальности информации и порядка обращения с конфиденциальной информацией;

– сообщать руководителю структурного подразделения (непосредственному руководителю) и Руководителю направления информационной безопасности (по электронной почте ibmon@astk-insur.ru) о фактах получения либо попытках посторонних лиц или организаций получить конфиденциальную информацию, о случаях несанкционированного доступа к конфиденциальной информации и ее распространения, а также о других причинах или создавшихся условиях возможной утечки конфиденциальной информации;

– незамедлительно сообщать руководителю структурного подразделения (непосредственному руководителю) обо всех случаях утраты служебных документов, носителей, печатей, штампов, бланков строгой отчетности, удостоверений, пропусков, ключей от сейфов и шкафов;

– соблюдать порядок использования конфиденциальной информации и обеспечивать ее защиту от посторонних лиц в процессе работы с ней;

– передавать при уходе в отпуск, убытии в командировку, увольнении или переходе на другую

должность имеющиеся у него сведения другому работнику только по указанию руководителя структурного подразделения;

– соблюдать при взаимодействии (в том числе, подготовке и направлении / передаче документов, либо их копий) с правоохранительными, налоговыми и другими органами по вопросам, касающимся деятельности Компании или клиентов, установленный законодательством Российской Федерации и внутренними нормативными документами Компании порядок предоставления информации и контролировать соблюдение правил работы с конфиденциальной информацией при ее передаче; при возникновении вопросов в отношении правил работы с указанными органами работники могут обратиться за консультацией к Директору по юридическим вопросам, Руководителю направления информационной безопасности.

– своевременно в установленном порядке уничтожать (или передавать на уничтожение) информацию, файлы, документы и носители информации с истекшим сроком хранения, если таковой установлен

– представлять в Руководителю направления информационной безопасности письменные объяснения, касающиеся нарушений требований, установленных настоящим Положением, а также о фактах утечки, хищения, утраты, искажения и разглашения конфиденциальной информации;

– предъявлять по требованию Руководителя направления информационной безопасности для проверки все имеющиеся материальные носители, содержащие конфиденциальную информацию.

5.2. Работникам Компании запрещается:

– разглашать сведения, составляющие конфиденциальную информацию, в том числе путем предоставления доступа к ней;

– разглашать конфиденциальную информацию, полученную в Компании в процессе выполнения должностных обязанностей, после перехода на другую должность или увольнения в течение срока, установленного трудовым договором, обязательством или дополнительным соглашением;

– использовать конфиденциальную информацию Компании при обмене информацией по незащищенным каналам связи и без соблюдения мер защиты;

– использовать конфиденциальную информацию, владельцем которой является Компания, в своих личных целях, а также в интересах других организаций, физических лиц, индивидуальных предпринимателей;

– использовать конфиденциальную информацию в открытой переписке, статьях и выступлениях и в личных интересах;

– снимать копии с документов или с других носителей информации, составляющих или содержащих конфиденциальную информацию, или производить выписки из них, а равно использовать любые технические средства для записи конфиденциальной информации, если это не предусмотрено функциональной задачей или должностными обязанностями;

– обсуждать конфиденциальную информацию с лицами, не имеющими доступа к такой информации (или в их присутствии), в том числе с друзьями, родственниками, работниками Компании, не допущенными к работе с данной информацией, посторонними лицами и т.п.;

– хранить электронные документы, содержащие конфиденциальную информацию, в общедоступных местах, включая общедоступные папки файловых серверов[3], внешние web и Интернет-ресурсы и т.п.

– публиковать материалы, содержащие конфиденциальную информацию, в открытой печати,

[3] В отношении которых нет разграничения доступа

использовать в передачах по радио, телевидению и компьютерным сетям, в публичных выступлениях без соответствующего разрешения Руководства Компании;

– оставлять документы и носители, содержащие конфиденциальную информацию на столах при отсутствии на рабочем месте, в незакрытых на замок сейфах (шкафах);

– осуществлять обработку конфиденциальной информацией с использованием личных и неавторизованных устройств, на которые не распространяются средства защиты информации.

6. Порядок работы с конфиденциальной информацией и обращения с документами, содержащими конфиденциальную информацию

6.1. Доступ Пользователей к конфиденциальной информации должен осуществляться в соответствии с п.3 настоящего Положения.

6.2. Хранение конфиденциальной информации (обработка – для информации в электронном виде), осуществляется Компанией:

− в помещениях и хранилищах, обеспечивающих ограничение доступа к конфиденциальным сведениям;

− в электронных хранилищах (базах данных) информации (серверы, персональные компьютеры, ноутбуки, внешние носители информации и т.п.).

Размещение помещений и их оборудование должно исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность в этих помещениях документов и носителей.

6.3. Внутренняя планировка и расположение рабочих мест в помещениях, в которых осуществляется работа с конфиденциальной информацией, должны осуществляться с учетом обеспечения персональной ответственности работников за сохранность вверенных им документов, содержащих конфиденциальную информацию.

Для хранения конфиденциальных документов указанные помещения снабжаются необходимым количеством металлических или иных запирающихся шкафов.

6.4. Информационные активы, содержащие и составляющие конфиденциальную информацию, хранящиеся в электронных хранилищах и использующиеся в информационных системах Компании, должны быть защищены от несанкционированного копирования и доступа к ним. Должны быть обеспечены конфиденциальность этих активов, целостность и доступность. Предоставление доступа к конфиденциальной информации, обрабатываемой в информационных системах, осуществляется в соответствии с п.3 настоящего Положения.

6.5. Передача конфиденциальной информации сторонним организациям, если иное не установлено законодательством Российской Федерации, должна регулироваться договорными отношениями, предусматривающими обязательства и ответственность сторон за разглашение конфиденциальной информации, ставшей известной в процессе взаимодействия.

6.6. Электронный обмен конфиденциальной информацией с третьими лицами должен осуществляться с использованием защищенных каналов связи, либо мер защиты и только уполномоченными сотрудниками Компании в соответствии с требованиями внутренних нормативных документов Компании.

6.7. Автоматизированные рабочие места (далее – АРМ) Пользователей, на которых обрабатывается конфиденциальная информация, должны быть оснащены средствами защиты информации.

6.8. При выводе АРМ Пользователя из использования или передачи на сервисное обслуживание (ремонт) конфиденциальная информация должна быть уничтожена.

6.9. Уничтожение конфиденциальной информации на АРМ Пользователей и носителях

конфиденциальной информации должно производиться Руководителем направления информационных технологий специальным программным обеспечением или с помощью средств гарантированного уничтожения информации.

6.10. Руководители структурных подразделений обязаны обеспечить хранение документов, содержащих конфиденциальную информацию, способом, исключающим возможность несанкционированного доступа третьих лиц к такой информации. Например, в отдельных папках в металлических или иных шкафах (сейфах, ящиках), запираемых на ключ.

6.11. Ответственность за сохранность документов, составляющих конфиденциальную информацию, хранящихся в структурных подразделениях Компании, несут руководители подразделений.

6.12. Передача в архив дел и документов, содержащих конфиденциальную информацию и утративших практическое значение, а также дальнейшее уничтожение архивных документов и дел[4] производится в соответствии с внутренними документами Компании, определяющими процедуры архивного делопроизводства.

6.13. Компания, являясь обладателем конфиденциальной информации, оставляет за собой право осуществлять протоколирование и мониторинг действий работников с конфиденциальной информацией и контролировать выполнение требований по соблюдению режима конфиденциальности информации со стороны Пользователей, в том числе, с использованием программно-технических средств. В случае нарушения работником политик Компании, определяющих допустимое использование информационных ресурсов в результате использования технических средств Компании и информационных ресурсов в личных целях Руководитель направления информационной безопасности может получить доступ к личным сведениям работника.

6.14. Контроль режима конфиденциальности информации и протоколирование действий осуществляются в целях изучения и оценки фактического состояния работы по обеспечению защиты и сохранности конфиденциальной информации, выявления недостатков и лиц, нарушающих установленный режим при работе с конфиденциальной информацией, установления причин таких недостатков и нарушений, и выработки предложений, направленных на устранение и предотвращение недостатков и нарушений.

Контроль режима конфиденциальности информации, включая режим работы с документами и носителями, содержащими конфиденциальную информацию, осуществляет Руководитель направления информационной безопасности и руководители соответствующих подразделений.

7. Порядок предоставления конфиденциальной информации сторонним организациям

7.1. Сведения, содержащие или составляющие конфиденциальную информацию Компании, могут быть предоставлены органам государственной власти, иным государственным органам, органам местного самоуправления, обладающим правом на получение конфиденциальной информации, в соответствии с действующим законодательством Российской Федерации. Конфиденциальная информация передается строго в пределах, необходимых для выполнения ими своих функций, и в соответствии с законодательством Российской Федерации.

7.2. Предоставление сведений, содержащих конфиденциальную информацию Компании, третьим лицам (юридическим лицам и физическим лицам, не являющимся работниками Компании) запрещается, за исключением случаев, определенных в п.3.5. и 7.1 настоящего Положения.

[4] Способом, обеспечивающим невозможность их восстановления

8. Ответственность за разглашение конфиденциальной информации, утрату документов содержащих такую информацию, и нарушение порядка работы с ними

8.1. Разглашение конфиденциальной информации, утрата документов, содержащих такую информацию, является инцидентом информационной безопасности (далее – инцидент ИБ[5]), который подлежит обработке в соответствии с внутренними политиками управления инцидентами информационной безопасностии влечет за собой ответственность, предусмотренную действующим законодательством Российской Федерации, в соответствии с договорными обязательствами между Компанией и Пользователем.

8.2. Результаты расследования сообщаются Руководству Компании в соответствии с внутренними политиками управления инцидентами информационной безопасности и содержат заключение с выводом для принятия решения руководством Компании о привлечении к ответственности работников, допустивших разглашение и утрату сведений, составляющих конфиденциальную информацию.

9. Функции структурных подразделений/должностных лиц Компании

9.1. Руководитель направления информационной безопасности:

– планирует мероприятия по защите конфиденциальной информации, организует их выполнение и контроль за их выполнением;

– участвует в разработке и внесении изменений во внутренние нормативные документы и процессы Компании, связанные с обработкой и защитой конфиденциальной информации;

– организует разработку и актуализацию (совместно со структурными подразделениями Компании) Перечня сведений, составляющих конфиденциальную информацию Компании;

– организует работы по оценке защищенности информационных ресурсов и разрабатывает предложения по повышению эффективности их защиты;

– изучает информационные, технологические и бизнес-процессы Компании с целью выявления, и закрытия возможных каналов несанкционированных распространения конфиденциальной информации и доступа к конфиденциальной информации, выявления возможных каналов утечки конфиденциальной информации и рисков, связанных с нарушением режима конфиденциальности информации;

– своевременно информирует Руководство Компании о рисках, связанных с хранением, использованием и обработкой конфиденциальной информации;

– осуществляет контроль, организацию разработки и реализации мер по защите конфиденциальной информации в соответствии с настоящим Положением;

– контролирует выполнение требований настоящего Положения в структурных подразделениях, в том числе по хранению и обращению с конфиденциальными документами;

– контролирует соблюдение правил работы с конфиденциальной информацией, в том числе, с применением программно-технических средств мониторинга;

– инициирует и принимает участие в проверках и расследованиях по фактам утечки и разглашения конфиденциальной информации, несанкционированного распространения и доступа к конфиденциальной информации, по другим инцидентам в области защиты конфиденциальной информации, а также в разработке предложений по устранению недостатков и предупреждению подобного рода нарушений;

– вырабатывает предложения по созданию и совершенствованию систем защиты

[5] Определение см. в Политикой управления инцидентами информационной безопасности ООО Страховая компания «АСТК»

конфиденциальной информации;

– организовывает работы по выбору, внедрению, приемке, настройке и вводу в эксплуатацию средств защиты информации;

– проводит консультации и инструктажи с руководителями и сотрудниками подразделений Компании, допущенными к работе с конфиденциальной информацией, по вопросам методов защиты и правил работы с указанной информацией для обеспечения ее сохранности;

– взаимодействует с Пользователями по вопросам защиты конфиденциальной информации.

9.2. Руководитель направления информационных технологий:

− участвуют в определении требований к обработке и защите конфиденциальной информации;

− обеспечивает контроль соблюдения правил работы с конфиденциальной информацией посредством разграничения доступа к информационным ресурсам и обеспечивает управление правами доступа к информационным ресурсам Компании в соответствии с приказами по Компании, утвержденными документами, относящимися к сфере информационной безопасности;

− консультируют работников Компании по вопросам соблюдения правил работы на компьютерах;

− осуществляют ликвидацию (уничтожение) конфиденциальной информации на магнитных носителях при необходимости (при передаче их из подразделения в подразделение, при продаже, отправке в ремонт и т.п.);

− предоставляют Руководителю направления информационной безопасности сведения о выявленных нарушениях правил работы с конфиденциальной информацией;

− поддерживают технические средства защиты информации в рабочем состоянии;

− совместно с Руководителем направления информационной безопасности участвуют в работах по выбору, внедрению, приемке, настройке и вводу в эксплуатацию средств защиты;

− совместно с Руководителем направления информационной безопасности осуществляют внедрение и настройку средств защиты;

− участвуют в работах по оценке защищенности информационных ресурсов, выявлении каналов утечки конфиденциальной информации и разработке предложений по повышению эффективности защиты;

− участвуют в расследованиях в области защиты конфиденциальной информации, разработке предложений по устранению недостатков и предупреждению подобного рода нарушений;

− участвуют в разработке и внесении изменений во внутренние нормативные документы и процессы Компании, связанные с обработкой и защитой конфиденциальной информации.

9.3. Руководитель направления по работе с персоналом:

− при приеме на работу доводит до работников требования внутренних нормативных документов Компании по вопросам обработки и защиты конфиденциальной информации под подпись[6] и обеспечивает своевременное оформление работниками Компании обязательств о неразглашении конфиденциальной информации;

− обеспечивает своевременное информирование Руководителя направления по информационной безопасности и Руководителя направления информационных технологий об увольнении или переводе работников в другие структурные подразделения Компании и связанной с этим необходимости изменения прав доступа к конфиденциальной информации.

9.4. Руководители структурных подразделений:

− обеспечивают ознакомление работников структурных подразделений с требованиями настоящего Положения;

[6] Либо путем ознакомления с документами в электронном виде с использованием корпоративного портала или информационной системы.

− обеспечивают и контролируют соблюдение правил работы с конфиденциальной информацией в подчиненных подразделениях;

− вносят предложения по включению / исключению информации в / из Перечня сведений, составляющих конфиденциальную информацию;

− обеспечивают защиту использующейся в процессе деятельности конфиденциальной информации;

− вносят предложения по совершенствованию системы защиты конфиденциальной информации;

− организуют внесение изменений в должностные инструкции и дополнительные документы, определяющие права и обязанности Пользователей в части обработки и обеспечения безопасности конфиденциальной информации;

− взаимодействуют с Руководителем направления по информационной безопасности при разработке мероприятий, направленных на защиту конфиденциальной информации в подчиненном подразделении;

− информируют Руководителя направления по информационной безопасности о нарушениях правил работы с конфиденциальной информацией в подчиненном подразделении.

9.5. Пользователи:

− соблюдают установленный Компанией режим конфиденциальности информации и выполняют все требования настоящего Положения.

10. Ответственность

10.1. Нарушение настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

10.2. Ответственность за организацию работ по обеспечению защиты конфиденциальной информации и контроль выполнения требований настоящего Положения в структурных подразделениях несет Руководитель направления по информационной безопасности.

10.3. Ответственность за выполнение обязанностей по обеспечению защиты конфиденциальной информации, возложенных на структурные подразделения, несут руководители соответствующих подразделений и работники данных подразделений.

10.4. Персональную ответственность за определение наличия и классификацию конфиденциальной информации, обеспечение сохранности конфиденциальной информации Компании несет каждый работник, принявший на себя обязательство о неразглашении конфиденциальной информации, в соответствии с действующим законодательством Российской Федерации и принятым им обязательством.

10.5. При выявлении нарушений требований к порядку обращения с конфиденциальной информацией, к работнику, допустившему нарушение, могут быть применены меры дисциплинарного взыскания.

10.6. При наличии признаков преступления в действиях лица, разгласившего конфиденциальную информацию, или допустившего утрату документов, содержащих такую информацию, Компания имеет право обращения в правоохранительные органы для привлечения его к ответственности в соответствии с действующим законодательством Российской Федерации.

10.7. При причинении лицом, разгласившим конфиденциальную информацию, вреда (экономического, морального и др.) и при отказе добровольно возместить ущерб, Компания имеет право обратиться в суд для защиты своих интересов.

10.8. Иные права, обязанности и ответственность Пользователей определяются должностными

инструкциями, внутренними нормативными документами Компании и действующим законодательством Российской Федерации.

11. Пересмотр документа

11.1. Пересмотр настоящего Положения проводится не реже одного раза в 3 года, а также:

– при изменении законодательства, связанного с обеспечением ИБ конфиденциальной информации;

– при внесении в организационно-функциональную структуру Компании изменений, касающихся структурных подразделений, задействованных в реализации настоящего Положения;

– по решению руководства Компании.

Под пересмотром документа понимается проверка соответствия положений документа требованиям нормативных документов Компании, требованиям стандартов, требованиям бизнес-деятельности и т.п. Пересмотр документа не подразумевает обязательного внесения каких-либо изменений в документ.

11.2. Пересмотр настоящего Положения производится Руководителем направления по информационной безопасности с привлечением, при необходимости, работников других структурных подразделений Компании.

Приложение 1
к Положению о защите конфиденциальной информации в ООО Страховая компания «АСТК»

Перечень сведений, составляющих конфиденциальную информацию ООО Страховая компания «АСТК»

1. Сведения, составляющие страховую тайну

Сведения о страхователях, застрахованных лицах и выгодоприобретателя, в том числе:

1.1. Сведения о страхователях, застрахованных лицах и выгодоприобретателя, страховых агентах, брокерах, сведения о взаимоотношениях с ними, их финансовом положении, проводимых операциях и объемах.

1.2. Условия действующих и заключаемых договоров, данные о размере полученной страховой премии, комиссии и оплаченных убытках.

1.3. Сведения о предоставленных Компанией продуктах, услугах и условиям по ним.

1.4. Сведения о состоянии их здоровья, а также об имущественном положении этих лиц.

1.5. Сведения о коммерческих предложениях потенциальным клиентам.

1.6. Сведения из документов, предоставленных клиентом или в отношении клиента, страхователя или застрахованного лица, документов, формируемых в ходе взаимоотношений с клиентом.

1.7. Сведения, содержащие номера банковских карт клиентов и иные данные платежных карт[7], номера банковских счетов и их реквизиты.

1.8. Сведения об отношениях между Компанией и клиентом, в том числе о том, ведутся или велись переговоры между Компанией и клиентом.

2. Персональные данные

Информация, содержащая персональные данные работников и третьих лиц и не являющаяся общедоступной в соответствии с Законодательством Российской Федерации[8].

3. Коммерческая тайна

Информация, составляющая коммерческую тайну Компании и третьих лиц и не являющаяся общедоступной в соответствии с Законодательством Российской Федерации[9].

4. Конфиденциальная информация, определенная Внутренним стандартом Всероссийского союза страховщиков «Обеспечение защиты конфиденциальной информации при осуществлении страховой деятельности»

4.1. Сведения об объектах страхования, обладателями которых являются стратегические предприятия и акционерные общества, определенные Указом Президента Российской Федерации от 04 августа 2004 года № 1009.

4.2. Сведения об объектах страхования, относящихся к товарам двойного назначения, определенным Постановлением Правительства РФ от 19.07.2022 № 1299 «Об утверждении списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль».

---

[7] Основной номер держателя карты (PAN), имя держателя карты, дата истечения срока действия карты, сервисный код, полные данные дорожки магнитной полосы или ее эквивалент на чипе, CAV2/CVC2/CVV2/CID, PIN/PIN-блоки.

[8] Полный перечень персональных данных, обрабатываемых в Компании и составляющих конфиденциальную информацию Компании, определяется во внутренних нормативных документах Компании.

[9] Полный перечень сведений, составляющих коммерческую тайну Компании и обрабатываемых в Компании, определяется во внутренних нормативных документах Компании.

4.3. Сведения об имущественных интересах граждан и организаций Российской Федерации, находящихся под действием иностранных санкций.

4.4. Сведения о вооружении, военной технике, объектах военно-промышленного комплекса Российской Федерации и государственного оборонного заказа, о воинских перевозках и транспортировке особо опасных грузов, включая наименование, количество, стоимость, дислокацию, маршруты и способы транспортировки.

4.5. Сведения об ущербе и происшествиях, которые произошли в отношении имущественных интересов граждан и организаций Российской Федерации, находящихся под действием иностранных санкций.

4.6. Сведения об ущербе и происшествиях, которые произошли в отношении вооружения, военной техники, объектов военно-промышленного комплекса Российской Федерации и государственного оборонного заказа, воинских перевозок и транспортировок особо опасных грузов.

5. Иная конфиденциальная информация

5.1. Сведения о целях, задачах и тактике переговоров с клиентами и деловыми партнерами, сведения о подготовке и результатах проведения таких переговоров.

5.2. Сведения о клиентах, инвесторах, посредниках и других партнерах, которые не содержатся в открытых источниках (справочниках, каталогах и др.) или переданы Компании указанными лицами на доверительной основе (в том числе адреса, телефоны, сведения об имущественных правах, аффилированных лицах, деловых связях и т.п.).

5.3. Сведения об условиях, заключенных или планируемых договоров /контрактов, в т.ч. договоров с клиентами, их содержании, размерах и порядке выплат.

5.4. Сведения о взаиморасчетах между Компанией и ее контрагентами / клиентами.

5.5. Сведения о финансово-хозяйственной, экономической и инвестиционной деятельности Компании, о состоянии учредителей, партнеров и участников Компании.

5.6. Сведения о персональном доходе и вознаграждении работников Компании.

5.7. Показатели выполнения финансового плана по Компании и в разрезе отдельных направлений деятельности.

5.8. Сведения, содержащиеся во входящих документах, содержащих гриф конфиденциальности, конфиденциальная информация партнеров.

5.9. Сведения о планах развития компании: стратегические и тактические.

5.10. Сведения о планах рекламной деятельности.

5.11. Сведения о прибыльности и убыточности видов страхования.

5.12. Сведения о страховых продуктах, методике продаж страховых продуктов, планы по продвижению и разработке страховых продуктов.

5.13. Сведения о формах и методах работы с активами, о структуре инвестиционного портфеля Компании

5.14. Сведения о коммерческих и инновационных предложениях Компании.

5.15. Сведения о коммерческих замыслах.

5.16. Сведения о результатах маркетинговых исследований.

5.17. Сведения об эффективности коммерческой деятельности.

5.18. Сведения о конкретных направлениях и результатах в инвестиционной политике.

5.19. Сведения о фактах подготовки и ведения переговоров.

5.20. Сведения о мероприятиях, проводимых перед переговорами.

5.21. Протоколы заседаний Совета директоров.

5.22. Протоколы заседаний комитетов и коллегиальных органов Компании.

5.23. Сведения о фактах заключения договоров / сделок.

5.24. Информация / документация об исполнении / о ходе исполнения сделок и контрактов / о проблемах, возникающих при исполнении сделок, в том числе связанных с возникновением спорных ситуаций с контрагентами / государственными органами.

5.25. Сведения о паролях, кодах доступа к программным и техническим средствам, в том числе ключи средств криптографической защиты информации (СКЗИ), ключи электронной подписи, используемые в информационных системах, логины и пароли ко всем продуктам, предоставляемым клиентам в рамках обслуживания через системы электронного фронт-офиса.

5.26. Информация о конфигурациях, определяющих параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования.

5.27. Сведения об особенностях функционирования разрабатываемого и используемого в Компании программного обеспечения, в том числе исходные тексты программ, сведения об их архитектуре и алгоритмам взаимодействия с другими системами.

5.28. Сведения о системе, средствах и методах защиты информации, в том числе конкретные сведения о криптографических ключах, используемых для защиты информации в информационных системах, и данные технических проектов и документаций.

5.29. Сведения об организации физической защиты и пропускном режиме в Компании.

5.30. Сведения о результатах расследований и служебных проверок.

5.31. Сведения, содержащиеся в рабочих материалах, отчетах ревизий и проверок, проводимых в ходе процедур комплаенса и внутреннего контроля, внутреннего аудита, а также в рамках проверок внешних аудиторов и контролирующих органов.

5.32. Сведения, содержащиеся в переписке с надзорными органами и сторонними организациями, по вопросам контрольно-ревизионных проверок.

5.33. Сведения о событиях реализации операционного риска.

5.34. Внутренние документы Компании (приказы, регламенты, положения, инструкции, правила, процедуры, описания технологий и методик и др.).

5.35. Платежная информация, к которой относится:

– Информация об остатках денежных средств на банковских счетах Компании.
– Информация о совершенных переводах денежных средств.

Приложение 2
к Положению о защите конфиденциальной информации в ООО Страховая компания «АСТК»

ОБЯЗАТЕЛЬСТВО

о неразглашении конфиденциальной информации

Я, _____
(фамилия, имя, отчество)

являясь работником ООО Страховая компания «АСТК» (далее – Компания) в период трудовых отношений с ООО Страховая компания «АСТК» и после их окончания обязуюсь:

− не разглашать сведения, составляющие конфиденциальную информацию Компании и ее партнеров, которые мне будут доверены или станут известны в процессе работы;

− не передавать третьим лицам и не раскрывать сведения, составляющие конфиденциальную информацию Компании;

− выполнять относящиеся ко мне требования приказов, инструкций и положений внутренних нормативных документов по обеспечению сохранности и защиты конфиденциальной информации Компании;

− в случае попытки посторонних лиц получить от меня конфиденциальную информацию Компании или осуществить иные действия, направленные на нанесение ущерба ООО Страховая компания «АСТК», немедленно сообщить об этом своему непосредственному руководителю и руководителю Управления информационной безопасности;

− сохранять конфиденциальность информации тех предприятий и организаций, с которыми имеются деловые отношения Компании;

− не использовать знание конфиденциальной информации Компании для занятий любой деятельностью, которая может нанести ущерб Компании;

− не использовать знание конфиденциальной информации Компании, предприятий и организаций, с которыми имеются деловые отношения Компании, в своих личных целях, а также в интересах других организаций, физических лиц, индивидуальных предпринимателей;

− в случае моего увольнения все носители конфиденциальной информации (рукописи, черновики, чертежи, схемы, распечатки на принтерах, магнитные ленты, съемные носители информации и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Компании, передать своему непосредственному начальнику или другому работнику Компании по его указанию;

− об утрате или недостаче носителей конфиденциальной информации, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов) и других фактах, которые могут привести к разглашению конфиденциальной информации, а также о причинах и условиях возможной утечки сведений, немедленно сообщать своему непосредственному руководителю и руководителю Управления информационной безопасности.

В интересах обеспечения безопасности Компании я также даю согласие на проведение (в период трудовых отношений с Компанией) в отношении меня мероприятий и действий, направленных на охрану имущества и предотвращение распространения конфиденциальной информации, в том числе на осуществление протоколирования и мониторинга действий с конфиденциальной информацией с использованием программно-технических средств.

До моего сведения доведено с разъяснениями Положение о защите конфиденциальной информации ООО Страховая компания «АСТК» (далее – Положение).

Мне известно, что нарушение требований Положения и иных внутренних нормативных документов Компании может повлечь ответственность в соответствии с законодательством Российской Федерации.

« » ___ 20__ г. _____
(подпись) (ФИО)

Приложение 3
к Положению о защите конфиденциальной информации в ООО Страховая компания «АСТК»

ГРИФ «КОММЕРЧЕСКАЯ ТАЙНА»

КОММЕРЧЕСКАЯ ТАЙНА
Общество с ограниченной ответственностью Страховая компания «АСТК» (ООО Страховая компания «АСТК»)
105120, г. Москва, 2-ой Сыромятнический пер., д. 1, эт. 4, пом. 1, комн. 33-40