УТВЕРЖДЕНО
Приказом
Генерального директора
АО СГ «Спасские ворота»
от 28.06.2022 № 41/ОД

Политика
в отношении сбора, обработки, защиты персональных данных и информационной безопасности
в Акционерном обществе Страховая группа «Спасские ворота» (АО СГ «Спасские ворота»)

I. Общие положения

1.1 В целях применения настоящей Политики применяются следующие основные понятия:

"Автоматизированное рабочее место" (АРМ) – комплекс средств ЭВМ и программного обеспечения, располагающийся непосредственно на рабочем месте Работника и предназначенный для автоматизации его работы.

"Администратор ИСПДн" – Работник, уполномоченный на осуществление настройки и установку технических средств Информационной системы Персональных данных и обеспечение ее бесперебойной работу.

"Администратор ИСПДн Работников" – Работник, выполняющий функции Администратора ИСПДн применительно к Работникам.

"АС" – Автоматизированная система. АС относится к Информационной системе Персональных данных на основании следующих критериев:

- наличие в АС Персональных данных;
- возможность записи, систематизации, накопления, хранения, уничтожения Персональных данных;
- защита информации, предусмотренная требованиями законодательства.

"База данных" – совокупность систематизированных данных, хранимых в соответствии со схемой данных, данные которой могут быть найдены и обработаны с помощью ЭВМ.

"Биометрические Персональные данные" – сведения, характеризующие физиологические и биологические особенности человека и на основе, которых можно установить его личность и которые используются Оператором для установления личности Субъекта Персональных данных.

"Блокирование Персональных данных" - временное прекращение сбора, систематизации, накопления, использования, распространения Персональных данных работников, в том числе их передачи.

"Веб сайт" –сайт Оператора в сети Интернет https://spasskievorota.ru/.

"Выгодоприобретатель" – лицо, в пользу которого заключен договор страхования.

"Застрахованное лицо" – лицо, ответственность которого застрахована по договору страхования.

"Информационная безопасность" – комплекс мер, направленных на предотвращение несанкционированного доступа, использования, раскрытия, искажения, изменения, записи или уничтожения Персональных данных в Базе данных Оператора.

"Информационная система Персональных данных" – информационная система, представляющая собой совокупность Персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких Персональных данных с использованием средств автоматизации или без использования таких средств.

"Использование Персональных данных" - действия (операции) с Персональными данными, совершаемые должностным лицом Организации в целях принятия решений или

совершения иных действий, порождающих юридические последствия в отношении Субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

"Кандидат" означает физическое лицо, планирующее вступить в трудовые отношения с Работодателем.

"Конфиденциальность Персональных данных" – обязательное для соблюдения Оператором или иным уполномоченным Оператором лицом, получившим доступ к Персональным данным, требование не допускать их распространения без согласия Субъекта или наличия иного законного основания.

"Обезличивание Персональных данных" - действия, в результате которых невозможно определить принадлежность Персональных данных конкретному работнику.

"Обработка Персональных данных Субъекта" (перечень действий с Персональными данными на обработку которых Субъекта Персональных данных дает согласие) – любые действия с использованием средств автоматизации или без таковых (операции) с Персональными данными, включая получение, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, комбинирование, передачу (трансграничную передачу, распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение или любое другое использование Персональных данных Субъекта Персональных данных.

"Персональные данные Субъекта" (Персональные данные) – любая информация, относящаяся к Субъекту Персональных данных, на основе которой такой Субъект может быть определен, включая, но не ограничиваясь следующей информацией:

- биометрические данные,
- бывший в трудовых отношениях с Работодателем.
- год, месяц и дату рождения, место рождения,
- гражданство,
- данные о трудовой деятельности (включая опыт работы),
- данные об образовании, знании иностранных языков, данные по повышению квалификации и переподготовке,
- данные рабочей визы, паспортные данные или данные иного документа, удостоверяющего личность (включая серию и/или номер, дату выдачи и выдавший орган),
- должность,
- изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен).
- ИНН, номер свидетельства государственного пенсионного страхования,
- информация о заболеваниях субъекта, затрудняющих выполнение субъектом трудовой функции,
- контакты – адрес регистрации и фактический адрес проживания, адрес личной электронной почты,
- находящееся в трудовых отношениях с Работодателем;
- пол,
- рабочие контактные данные (включая адрес корпоративной электронной почты),
- сведения медицинского характера (в случаях, предусмотренных законом)
- сведения о заработной плате и иных доходах и выплатах, сведения о социальных льготах, декларациях, подаваемых в органы Федеральной налоговой службы РФ (в том числе территориальные), данные, направляемые в органы Федеральной службы государственной статистики (в том числе территориальные органы),
- сведения о наличии судимости и иные данные,
- сведения о семейном положении и составе семьи, воинском учете,
- табельный номер Работника,
- телефон (личный мобильный, домашний),
- фамилию, имя, отчество,

Персональные данные относятся к категории конфиденциальной информации

"ПО" означает программное обеспечение.

"Работник" означает физическое лицо, трудоустроенное у Оператора в соответствии с Трудовым кодексом Российской Федерации.

"Распространение Персональных данных" - действия, направленные на передачу Персональных данных работников определенному кругу лиц (передача Персональных данных) или на ознакомление с Персональными данными неограниченного круга лиц, в том числе обнародование Персональных данных Субъектов в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к Персональным данным работников каким-либо иным способом.

"Ресурс Персональных данных" – база данных Субъектов Персональных данных, объединенных общими целями обработки Персональных данных с использованием или без использования объектов автоматизации, в том числе АС. Единственным Ресурсом Персональных данных Оператора является Автоматизированная информационная система (АИС).

"Родственник работника" – родственники Работника по прямой восходящей или нисходящей линии (родители и дети, дедушки, бабушки и внуки).

"Страхователь" – юридическое лицо или дееспособное физическое лицо, заключившее с Оператором договор страхования.

"Страховой агент" – физическое или юридическое лицо, от имени и по поручению Оператора занимающееся заключением договоров страхования и их сопровождением.

"Страховой брокер" – самостоятельный субъект страхового рынка, осуществляющий брокерскую деятельность в области страхования и перестрахования от своего имени в интересах своих клиентов.

"Субъект Персональных данных" (также Субъект) – согласно пункту 1.2.1. Политики.

"Уничтожение Персональных данных" - действия, в результате которых невозможно восстановить содержание Персональных данных в информационной системе Персональных данных работников или в результате которых уничтожаются материальные носители Персональных данных Субъектов.

"ЭВМ" – электронно-вычислительная машина.

1.2 **Акционерное общество Страховая группа «Спасские ворота»** (далее – "Общество", "Работодатель" или "Оператор"), осуществляет работу с персональными данными субъектов персональных данных (далее – "Субъектов"), осуществляет обработку персональных данных Субъектов и их защиту от несанкционированного доступа, неправомерного использования или утраты и обеспечивает информационную безопасность, руководствуясь соответствующими нормами Конституции Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, а также общепризнанными принципами и нормами международного права и международных договоров РФ, которые в соответствии с ч. 4 ст. 15 Конституции РФ являются составной частью российской правовой системы.

1.2.1. Субъектами являются:

- Работник;
- Родственники работника;
- Страхователи;
- Застрахованные лица;
- Выгодоприобретатели;
- Страховые агенты;
- Страховые брокеры;
- Посетители сайта Оператора;
- лица, оказывающие услуги (выполняющие работы) по договору гражданско-правового характера;
- третьи лица, пострадавшие в результате наступления страхового случая;
- все физические лица, так или иначе взаимодействующие с Оператором, в том числе по заключенным договорам.

1.3 Настоящая Политика определяет политику Общества как оператора, осуществляющего обработку Персональных данных, в отношении обработки и защиты Персональных данных, а также регламентирует порядок организации и правила обеспечения Информационной безопасности Оператора.

1.4 Настоящая Политика разработано на основе и во исполнение Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 г. № 152-ФЗ "О персональных данных" (далее – "Закон о персональных данных"), Федерального закона от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" и иных нормативных актов законодательства РФ.

1.5 Документами, содержащими Персональные данные, являются:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о постановке на учет в налоговый орган и присвоении ИНН;
- документы воинского учета;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- личная карточка Работника;
- автобиография, резюме Кандидата, характеристики, рекомендательные письма и иные аналогичные документы;
- медицинское заключение о состоянии здоровья и листок нетрудоспособности;
- документы, содержащие сведения о заработной плате, доплатах, надбавках, компенсациях и льготах;
- приказы о приеме на работу, об увольнении, о переводе на другую должность, о поощрениях и взысканиях, о повышении заработной платы, премировании, об отпусках и иные приказы по личному составу;
- документы по командировкам и деловым встречам Работников;
- заявления, запросы, объяснительные, докладные и служебные записки Работников;
- документы (отчеты, заключения, акты, сообщения, информация, справки, переписка, докладные и служебные записки) о соблюдении дисциплины труда,
- трудовой договор и дополнения к нему;
- документы о достижениях Работника, его интервью, повышениях квалификации,
- штатное расписание;
- график отпусков;
- переписка по вопросам трудоустройства;
- разрешения на работу и иные документы, необходимые для оформления трудовых отношений с иностранными Субъектами Персональных данных;
- договоры страхования;
- договоры перестрахования;
- акты о страховом случае;
- материалы выплатного дела;
- агентские договоры, заключенные со страховыми агентами;
- брокерские договоры, заключенные со страховыми брокерами;
- договоры, заключаемые с третьими лицами;
- согласия Субъекта Персональных данных на обработку Персональных данных,
- иные документы, которые с учетом специфики работы и в соответствии с законодательством и локальными нормативными актами Работодателя должны быть предъявлены Субъекту Персональных данных при заключении трудового договора или в период его действия;
- другие документы и электронные носители, содержащие персональные сведения, предназначенные для использования уполномоченными Работниками Оператора в служебных целях.

1.6 Цели обработки Персональных данных:

- заключение трудовых договоров и исполнение трудовых договоров;
- содействие в трудоустройстве, обучении и продвижении по службе;
- обеспечение личной безопасности;
- контроль количества и качества выполняемой работы (включая аттестацию и оценку деятельности);
- расчет заработной платы, пособий и иных выплат;
- организация командировок и иных разъездов работников (включая компенсацию расходов);
- возможность связаться с Субъектом Персональных данных в случае служебной необходимости;
- осуществление технической и организационной поддержки Субъекта Персональных данных в служебных целях;
- обеспечение сохранности имущества Субъекта Персональных данных и Работодателя;
- обеспечение законных интересов Субъекта Персональных данных, связанных с трудовой деятельностью у Работодателя;
- заключение договоров страхования и их исполнение;
- оценка рисков по договору страхования;
- заключение и сопровождение договоров со страховыми брокерами и страховыми агентами;
- обеспечение сохранности имущества;
- урегулирование убытков;
- урегулирование договорных отношений со страховыми агентами и страховыми брокерами;
- осуществление рекламных рассылок;
- обеспечение обмена информацией в электронном виде между Страхователем (Застрахованным лицом, Выгодоприобретателем) и Страховщиком с использованием официального сайта Страховщика в информационно-телекоммуникационной сети «Интернет»;
- аутентификация и автоматическое управление учетными записями информационных систем и баз данных;
- оценка ущерба сторонними компаниями;
- мониторинг удовлетворенности клиентов;
- обработка обезличенных Персональных данных в статистических или иных исследовательских целях;
- реализация ликвидных остатков транспортных средств;
- перестрахование;
- участие страховых тендерах (закупочных процедурах);
- компенсация ущерба третьим лицам, пострадавшим при наступлении страхового случая;
- осуществление досудебной и судебной работы, в т.ч. в целях взыскания дебиторской задолженности;
- предоставление сведений уполномоченным органам, организациям в соответствии с требованиями законодательства РФ;
- взаимодействие и обмен информацией с Субъектом, в том числе путем осуществления прямых контактов с Субъектом с помощью средств связи по вопросам оказания и/или продвижения страховых услуг Оператора;
- предоставление пользователям Веб сайта доступа к сервисам, информации и/или материалам, содержащимся на Веб сайте;
- иные цели, направленные на обеспечение соблюдения законов и иных нормативных правовых актов.

1.7 При обработке Персональных данных Оператор обеспечивает соблюдение следующих принципов, установленных в ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

- законности и справедливости;
- ограничения обработки Персональных данных достижением конкретных, заранее определенных и законных целей, соответствия целей обработки Персональных данных целям сбора Персональных данных;
- соответствия объема и характера обрабатываемых Персональных данных, способов обработки Персональных данных целям обработки Персональных данных;
- достоверности Персональных данных, их достаточности для целей обработки и актуальности по отношению к целям обработки, недопустимости обработки Персональных данных, избыточных по отношению к заявленной цели их обработки;
- принятием необходимых мер (либо обеспечением их принятия) по удалению или уничтожению неполных или неточных Персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей обработки Баз данных, содержащих Персональные данные;
- уничтожения Персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- личной ответственности Работников Оператора за сохранность и конфиденциальность Персональных данных при их обработке, а также их материальных носителей;
- наличия четкой разрешительной системы доступа Работников Общества к документам и Базам данных, содержащих Персональные данные;
- хранения Персональных данных в форме, позволяющей определить Субъекта, не дольше, чем этого требуют цели обработки, если срок хранения Персональных данных не установлен федеральным законом, договором, стороной которого является Субъект.

1.8 Оператор осуществляет обработку персональных данных в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и уведомляет уполномоченный орган по защите прав Субъектов персональных данных об обработке их Персональных данных.

1.9 При обработке Персональных данных соблюдаются следующие принципы обработки Персональных данных:

- установление цели обработки Персональных данных;
- определение перечня и категорий обрабатываемых Персональных данных;
- выполнение процедур учета количества Субъектов Персональных данных, в том числе Субъектов Персональных данных, не являющихся Работниками;
- выполнение ограничения обработки Персональных данных достижением цели обработки Персональных данных;
- соответствие содержания и объема обрабатываемых Персональных данных установленным целям обработки;
- точность, достаточность и актуальность Персональных данных, в том числе по отношению к целям обработки Персональных данных;
- выполнение установленных процедур получения согласия Субъектов Персональных данных (их законных представителей) на обработку Персональных данных в случае, если получение такого согласия необходимо в соответствии с требованиями законодательства;
- выполнение установленных процедур получения согласия Субъектов Персональных данных не передачу обработки их Персональных данных третьим лицам в случае, если получение такого согласия необходимо в соответствии с требованиями законодательства;
- прекращение обработки Персональных данных и уничтожение либо обезличивание Персональных данных по достижении целей обработки, по

требованию субъекта Персональных данных в случаях, предусмотренных законодательством, в том числе при отзыве Субъектом Персональных данных согласия на обработку его Персональных данных.

II. Правила обработки Персональных данных Субъектов Персональных данных

2.1. Основные положения

2.1.1. При обработке Персональных данных Субъектов Персональных данных в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объема и содержания обрабатываемых Персональных данных должны строго учитываться положения Конституции Российской Федерации, Налогового кодекса Российской Федерации, Гражданского кодекса Российской Федерации и иных федеральных законов, а также международных договоров, имеющих юридическую силу на территории России.

2.1.2. Сроки обработки Персональных данных Субъекта Персональных данных определяются следующим образом:

2.1.2.1. В отношении Работника и Родственников работника - в соответствии со сроком действия трудового договора, заключенного с работником, а также требованиями законодательства и нормативных документов;

2.1.2.2. В отношении Страхователя, Застрахованного лица и Выгодоприобретателя – в течение 5 лет, если иной срок не определен в действующем договоре страхования, а также требованиями законодательства и нормативных документов;

2.1.2.3. В отношении Страховых агентов и Страховых брокеров – в соответствии со сроком действия договоров, заключенных с ними, а также требованиями законодательства и нормативных актов;

2.1.2.4. В отношении остальных лиц – в соответствии с требованиями законодательства и нормативных актов.

2.1.3. Субъект Персональных данных предоставляет свое письменное согласие на обработку своих биометрических Персональных данных (фотографий, видеоизображения, записи голоса), которая осуществляется Оператором для идентификации личности Субъекта Персональных данных в целях, указанных в пункте 1.6 настоящей Политики. Обработка таких Персональных данных может осуществляться без согласия Субъекта Персональных данных в случаях, предусмотренных российским законодательством.

2.1.4. Обработка биометрических Персональных данных (включая запись и последующее хранение изображения на видео, голоса на диктофоне и т. д.) одних Субъектов Персональных данных другими Субъектами Персональных данных допускается только с письменного согласия первых, за исключением лиц, указанных в разделе IV настоящей Политики. Силу письменного согласия на обработку Персональных данных приравнивается нажатие на кнопку «Даю согласие на обработку персональных данных» на Сайте.

2.1.5. Согласия Субъекта Персональных данных на обработку Персональных данных не требуется в следующих случаях:

- обработка Персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения Персональных данных и круг субъектов (в который входит Работник), Персональные данные которых подлежат обработке, а также определяющего полномочия Работодателя как Оператора Персональных данных,
- обработка Персональных данных осуществляется в целях исполнения трудового договора,
- обработка Персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания Персональных данных,
- обработка Персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов Субъекта Персональных данных, если получение согласия Субъекта Персональных данных невозможно,

• обработка Персональных данных необходима для доставки почтовых отправлений организациями почтовой связи,

• в иных случаях, установленных в Законе о персональных данных.

• в случае служебной необходимости Субъект Персональных данных дает свое согласие на обработку Персональных данных по форме, установленной Работодателем.

2.2. Получение Персональных данных Субъекта Персональных данных.

2.2.1. Персональные данные Субъекта Персональных данных Оператор получает непосредственно от Субъекта Персональных данных. Оператор вправе получать Персональные данные Субъекта Персональных данных от третьих лиц только при уведомлении об этом Субъекта Персональных данных и при наличии письменного согласия Субъекта Персональных данных.

2.2.2. Сбор Персональных данных Субъекта персональных данных осуществляется путем:

• копирования оригиналов документов Субъекта Персональных данных;

• внесения сведений в учетные формы Работодателя (на бумажных и электронных носителях);

• внесения сведений о страхователях, застрахованном лице и выгодоприобретателях с помощью Личного кабинета Общества;

• получения / создания оригиналов необходимых документов (включая трудовую книжку, личную карточку Работника);

• заключения договоров страхования и перестрахования;

• урегулирования убытков;

• заключения иных договоров с третьими лицами;

• также на Веб сайте осуществляется обезличенная обработка Персональных данных о посетителях (в т.ч. файлов cookie) с использованием сервисов интернет-статистики (Яндекс Метрика, Гугл Аналитика и других сервисов).

2.2.3. Субъект Персональных данных представляет необходимые сведения и в случае необходимости предъявляет Оператору документы, подтверждающие достоверность этих сведений.

2.2.4. Оператор не вправе требовать от Субъекта Персональных данных предоставления информации о политических и религиозных убеждениях, а также о частной жизни Субъекта Персональных данных за исключением случаев, непосредственно связанных с вопросами трудовых отношений или страховых обязательств.

2.2.5. Оператор также не может запрашивать информацию о состоянии здоровья Субъекта Персональных данных за исключением тех сведений, которые относятся к вопросу о возможности выполнения Субъектом Персональных данных трудовой функции или выполнения обязательств Обществом перед субъектом Персональных данных.

2.3. Хранение Персональных данных.

2.3.1.1. Сведения, содержащие Персональные данные Работника, включаются в его личное дело, личную карточку Работника (применительно к Работникам и Родственникам работников), иные документы, а также содержатся на электронных носителях и в Базах данных Оператора, доступ к которым разрешен лицам, непосредственно использующим Персональные данные Работника в служебных целях. Перечень таких лиц определен в разделе IV настоящей Политики.

2.3.1.2. Сведения, содержащие персональные данные лиц, не являющихся работниками Общества включаются в личную карточку субъекта персональных данных, хранящуюся в базах данных Оператора и/или на физических носителях, доступ к которым разрешен лицам, непосредственно использующим Персональные данные Работника в служебных целях. Перечень таких лиц определен в разделе IV настоящей Политики.

2.3.2. Личное дело Работника, договоры страхования, иные договоры и документы, включающие в себя Персональные данные Субъекта, содержащиеся на бумажных носителях, находятся у Оператора в специально отведенном шкафу, который обеспечивает защиту от

несанкционированного доступа. Персональные данные Субъектов также хранятся в электронном виде в Базе данных на сервере Оператора, защищенном от несанкционированного доступа с помощью системы защиты, созданной в соответствии с разделом IV Политики. Ведение личных дел Работников возложено на работников отдела кадров Оператора. Хранение документов, содержащих Персональные данные Работников, осуществляется в течение сроков и в порядке, предусмотренными законодательством Российской Федерации

2.3.3. Персональных данные иных Субъектов хранятся в Базе данных на сервере Оператора.

2.4. Использование Персональных данных Субъектов Персональных данных, являющихся Работниками Общества.

2.4.1 Персональные данные Работника используются для целей, связанных с выполнением Работником трудовой функции. В частности, Работодатель использует Персональные данные Работника для решения вопросов продвижения Работника по службе, очередности предоставления ежегодного отпуска, установления размера заработной платы, премирования, направления Работника в служебные командировки, оформления льгот и т. д.

2.4.2. При принятии решений, порождающих юридические последствия в отношении Работника, Работодатель не имеет права основываться на Персональных данных Работника, полученных исключительно в результате их автоматизированной обработки или электронного получения, без получения на это письменного согласия Работника.

2.4.3. Использование и хранение биометрических Персональных данных Работника вне информационных систем Персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

2.5. Передача Персональных данных Субъекта Персональных данных.

2.5.1. Информация, относящаяся к Персональным данным Субъекта Персональных данных, может быть предоставлена государственным органам и негосударственным структурам в порядке, предусмотренном федеральным законодательством Российской Федерации. К таким органам и структурам, в частности относятся:

- Налоговые органы;
- Правоохранительные и судебные органы;
- Органы статистики;
- Военкоматы;
- Фонд Социального Страхования и его территориальные органы;
- Фонд Обязательного Медицинского Страхования и его территориальные органы;
- Пенсионный Фонд России и его территориальные органы;
- Федеральная Миграционная Служба и ее территориальные органы;
- Органы занятости населения;
- Муниципальные органы управления;
- Иные органы, которым в силу законодательства Работодатель должен предоставлять Персональные данные Субъекта Персональных данных исключительно в пределах, обусловленных целью их обработки и предусмотренных российским законодательством.

Такая информация передается по запросу вышеуказанных органов на основании настоящей Политики в случаях, предусмотренных российским законодательством.

2.5.2. Оператор может осуществлять передачу Персональных данных Субъекта Персональных данных партнерам и заказчикам, с которыми взаимодействует Оператор в процессе осуществления основной деятельности, которые приобретают услуги Оператора и в виду этого нуждаются в получении определенной информации в отношении Субъекта Персональных данных Оператора, вовлеченных в процесс оказания услуг и их маркетингового продвижения для целей оценки того, насколько Оператор и Субъекты Персональных данных подходят им для оказания услуг и предложения услуг, а также для целей обеспечения безопасности и защиты их собственности. При этом передаче подлежат только те

Персональные данные Субъекта Персональных данных, которые необходимы для осуществления вышеуказанных целей, а также иных целей, отвечающих требованиям законодательства.

2.5.3. Оператор не вправе предоставлять Персональные данные Субъекта Персональных данных третьей стороне без письменного согласия Субъекта Персональных данных, за исключением случаев, установленных федеральными законами.

2.5.4. В случае если лицо, обратившееся с запросом о получении Персональных данных, не уполномочено федеральным законом или иными правовыми актами на получение такой информации, либо отсутствует письменное согласие Субъекта Персональных данных на предоставление его Персональных данных, Оператор обязан отказать такому лицу. Лицу, обратившемуся с письменным запросом, может выдаваться письменное уведомление об отказе в предоставлении Персональных данных.

2.5.5. Персональные данные Субъекта Персональных данных могут быть переданы уполномоченным представителям Субъекта Персональных данных в порядке, установленном законодательством и только в том объеме, в котором они необходимы для выполнения указанными представителями их функции.

2.5.6. В случае, если Оператор на основании договора поручает обработку Персональных данных другому лицу, в том числе представителям Субъекта Персональных данных, в порядке, установленном Трудовым кодексом Российской Федерации и настоящей Политикой, то такое лицо обязано обеспечить конфиденциальность и безопасность Персональных данных Субъекта Персональных данных. Оператор должен ограничивать передачу такой информации только теми Персональными данными Работников и иных субъектов персональных данных, которые необходимы для выполнения третьими лицами их функций.

2.6. Обработка Персональных данных прекращается в следующих случаях:

2.6.1. При достижении целей обработки Персональных данных (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект Персональных данных, иным соглашением между Оператором и Субъектом Персональных данных);

2.6.2. Отзыва Субъектом Персональных данных согласия на обработку его Персональных данных, если сохранение Персональных данных более не требуется для целей обработки Персональных данных (если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект Персональных данных, иным соглашением между Оператором и Субъектом Персональных данных);

2.6.3. Если персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;

2.6.4. Выявления неправомерной обработки Персональных данных, осуществляемой Оператором, если обеспечить правомерность обработки Персональных данных невозможно;

2.6.5. Выявления неправомерной обработки Персональных данных без согласия Субъекта Персональных данных.

2.7. Хранение Персональных данных осуществляется в форме, позволяющей определить Субъекта Персональных данных не дольше, чем этого требуют цели обработки Персональных данных, если срок хранения Персональных данных не установлен законодательством, договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект Персональных данных.

2.8. Общедоступные источники Персональных данных могут создаваться и публиковаться Оператором только для цели выполнения требований законодательства.

2.9. Способы обработки Персональных данных Субъекта Персональных данных.

Обработка персональных данных Субъекта персональных данных осуществляется путем смешанной (как автоматизированной, так и неавтоматизированной) обработки, в том числе, с использованием внутренней сети и сети Интернет.

2.10. Меры по обеспечению безопасности Персональных данных при их обработке, осуществляемой без использования средств автоматизации:

2.10.1. Обработка Персональных данных, осуществляемая без использования средств автоматизации осуществляется таким образом, что в отношении каждой категории Персональных данных можно определить места хранения Персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку Персональных данных либо имеющих к ним доступ.

2.10.2. Раздельное хранение Персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

2.10.3. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность Персональных данных и исключающие несанкционированный к ним доступ.

2.11. В работе Веб сайта Оператора задействованы, в том числе, технологии cookie и веб-маяки (webbeacons). Указанные технологии позволяют предоставлять пользователям Сайта настроенное под них окружение при повторном посещении Веб сайта.

2.12. Cookie, используемые на Веб сайте, подразделяются на такие категории как: «необходимые», «эксплуатационные» и «функциональные».

2.12.1. Необходимые cookie обязательны для просмотра веб-страниц Веб сайта и полноценного использования их функций. Без их использования невозможно обеспечить работу таких сервисов как интернет-оплата, а также обеспечивается возможность авторизации пользователей на сайте.

2.12.2. Эксплуатационные cookie собирают информацию об использовании Веб сайта, например, о наиболее часто посещаемых его страницах. Указанные используются для оптимизации работы Веб сайта и упрощения для пользователей навигации по нему. Эксплуатационные cookie также используются аффилированными лицами Компании в целях определения переходов пользователей на Веб сайт с сайтов аффилированных лиц, а также определения использования сервисов Оператора, таких как осуществление онлайн-покупок в результате посещения Веб сайта. Вся информация, собранная с помощью cookie предназначена для статистических целей и остается анонимной.

2.12.3. Функциональные cookie позволяют Веб сайту запоминать пользовательский выбор при использовании Веб сайта. Такие cookie могут запоминать месторасположение пользователей для отображения Веб сайта на языке страны, в которой располагается пользователь, а также запоминать настройки размера шрифта текста и других настраиваемых параметров Веб сайта.

2.13. Информация, собираемая посредством cookie, не позволяет однозначно идентифицировать пользователей Веб сайта.

2.14. Если пользователи Веб сайта предпочитают не получать cookie при просмотре Веб сайта, они могут настроить свой браузер таким образом, чтобы не получать такие cookie, либо так, чтобы браузер предупреждал пользователей перед принятием cookie либо блокировал их.

III. Правовое основание обработки Персональных данных

3.1. Правовыми основаниями обработки Персональных данных Оператором являются:

- Согласие Субъекта на обработку его Персональных данных;
- Конституция РФ;
- Налоговый кодекс РФ;
- Трудовой кодекс РФ;
- Гражданский кодекс РФ;
- Закон РФ от 27.11.1992 № 4015-1 «Об организации страхового дела в РФ»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 25.04.2002 № 40-ФЗ «Об обязательном страховании гражданской ответственности владельцев транспортных средств»;
- Федеральный закон от 27.07.2010 № 225-ФЗ «Об обязательном страховании гражданской ответственности владельца опасного объекта за причинение вреда в результате аварии на опасном объекте»;
- Федеральный закон от 07.02.1992 № 2300-1 «О защите прав потребителей»;

- Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма»;
- Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»;
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в РФ»;
- Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ»;
- Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»;
- Федеральный закон от 26.02.1997 № 31-ФЗ «О мобилизационной подготовке и мобилизации в РФ»;
- Федеральный закон от 26.12.1995 № 208-ФЗ «Об акционерных обществах»;
- Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;
- Федеральный закон от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда»;
- Федеральный закон от 31.05.1996 № 61-ФЗ «Об обороне»;
- Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму»;
- Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в РФ»;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральных закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Положение ЦБ РФ от 16.11.2016 № 558-П «О правилах формирования страховых резервов по страхованию иному, чем страхование жизни»;
- Приказ Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;
- Приказ Минсоцразвития от 24.02.2005 № 160 «Об определении степени тяжести повреждения здоровья при несчастных случаях на производстве»

IV. Доступ к Персональным данным

4.1. Уполномоченные лица имеют право получать только те Персональные данные Субъекта Персональных данных, которые необходимы для выполнения их должностных обязанностей и функций. Все остальные Субъекты Персональных данных имеют право на полную информацию только об их Персональных данных и обработке этих данных.

4.2. Получение Персональных данных Субъекта Персональных данных третьей стороной без его письменного согласия возможно в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровья Субъекта персональных данных, а также в случаях, установленных федеральным законодательством.

4.3. Доступ к Персональным данным Работника как Субъекта Персональных данных имеют следующие должностные лица:

- Генеральный директор;
- Главный бухгалтер;
- Руководитель отдела кадров;
- Сотрудники отдела кадров;
- Субъект Персональных данных (в отношении своих Персональных данных).

4.4. Доступ к Персональным данным остальных Субъектов Персональных данных имеют следующие должностные лица:

- Генеральный директор;
- Главный бухгалтер;
- Работники, в трудовую функцию которых входит работа с персональными данными;

- Субъект персональных данных (в отношении своих Персональных данных).

4.5. Субъекты Персональных данных, доступ которых к Персональным данным, обрабатываемым в информационных системах Персональных данных, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим Персональным данным на основании списка, утвержденного Оператором.

V. Защита Персональных данных.

5.1. Под защитой Персональных данных понимается ряд правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

5.2. При передаче Персональных данных Субъекта Персональных данных с соблюдением условий, предусмотренных в настоящей Политике, Работники Оператора обязаны предупредить лиц, которым передаются данные, об ответственности в соответствии с законодательством Российской Федерации.

5.3. Защита информации осуществляется в соответствии с требованиями международных договоров, локальным нормативным актом Оператора в сфере защиты информации, требованиями Работодателя, а также российским законодательством.

5.4. Для защиты Персональных данных Субъекта Персональных данных Оператор обязан соблюдать следующие правила:

- ограничение и регламентация состава лиц, функциональные обязанности которых требуют доступа к информации, содержащей Персональные данные;
- избирательное и обоснованное распределение документов и информации, содержащих Персональные данные Субъектов Персональных данных, между лицами, функциональные обязанности которых требуют доступа к информации, содержащей Персональные данные;
- в помещениях Работодателя должны быть обеспечены необходимые условия для работы с конфиденциальными документами и базами данных, в том числе содержащими Персональные данные (в частности, для хранения документов, содержащих Персональные данные должны использоваться специально оборудованные шкафы или сейфы, которые запираются на ключ);
- должен быть организован порядок уничтожения информации, содержащей Персональные данные Субъекта Персональных данных, если законодательством не установлены требования по хранению соответствующих данных (в частности, бумажные носители, содержащие Персональные данные должны уничтожаться путем использования шредера или иным аналогичным способом);
- с Работниками должна производиться разъяснительная работа по предупреждению утраты сведений при работе с конфиденциальными документами (в том числе, документами, содержащими Персональные данные);
- личные дела Работников могут выдаваться только специально уполномоченным должностным лицам;
- персональные компьютеры, на которых содержатся Персональные данные, должны быть защищены паролями доступа;
- соблюдение порядка приема, учета и контроля деятельности посетителей на территории Работодателя;
- контроль соблюдения требований по обеспечению безопасности Персональных данных (путем проведения внутренних проверок, установления специальных средств мониторинга и др.);

• расследование случаев несанкционированного доступа или разглашения Персональных данных и привлечение виновных лиц к ответственности;
• иные требования, предусмотренные законодательством.

5.5. Оператор при обработке Персональных данных принимает необходимые правовые, организационные и технические меры, в том числе:

5.5.1. определяет угрозы безопасности Персональных данных при их обработке;

5.5.2. применяет организационные и технические меры по обеспечению безопасности Персональных данных, необходимые для выполнения требований к защите Персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности Персональных данных.

5.5.3. оценивает эффективность принимаемых мер по обеспечению безопасности Персональных данных.

5.5.4. обнаруживает факты несанкционированного доступа к Персональных данным и принимает меры, необходимые для предотвращения несанкционированного доступа и защиты Персональных данных.

5.5.5. восстанавливает Персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним.

VI. Способы защиты Персональных данных. Информационная безопасность

6.1. Внутренняя защита.

6.1.1. Основным виновным лицом несанкционированного доступа к Персональным данным, как правило, является Работник Оператора, работающий с документами и Базами данных, содержащими Персональные данные Субъектов. Регламентация доступа Работников Оператора к конфиденциальным сведениям, документам и Базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между Работниками Оператора.

6.1.2. Для обеспечения внутренней защиты Персональных данных Оператором соблюдаются следующие меры:

• ограничение состава Работников Оператора, функциональные обязанности которых требуют доступа к Персональным данным;
• строгое избирательное и обоснованное распределение документов и информации между Работниками Оператора;
• не допускается хранение документов, содержащий Персональные данные, на рабочих местах Работников после окончания обработки информации о Субъекта, либо при отсрочке обработки данных;
• рациональное размещение рабочих мест Работников, исключающее бесконтрольное использование защищаемой информации;
• наличие необходимых условий в помещении Оператора для работы с конфиденциальными документами и Базами данных;
• определение состава Работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
• организация порядка уничтожения информации;
• своевременное выявление нарушения требований разрешительной системы доступа Работниками соответствующего подразделения;
• разъяснительная работа с Работниками по предупреждению утраты ценных сведений при работе с документами и Базами данных, содержащими Персональные данные.

6.2. Внешняя защита.

6.2.1. Для защиты конфиденциальной информации от несанкционированного доступа к ней сторонних лиц создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для таких лиц. Целью и результатом несанкционированного доступа к Персональным данным может быть не только овладение ценными сведениями и их

использование, но и их видоизменение, уничтожение, заражение вирусом, подмена, фальсификация содержания документов и иные неблагоприятные последствия.

6.2.2. Под сторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Оператора, посетители Веб сайта. Посторонние лица не должны знать распределение функций Оператора, его рабочие процессы, технологию составления, оформления, ведения и хранения документов.

6.2.3. Для обеспечения внешней защиты Персональных данных необходимо соблюдать ряд мер:

- пропускной режим Оператора;
- исправность технических средств охраны, сигнализации;
- требования к защите информации при интервьюировании и собеседованиях.

6.3. Организационная система защиты информации.

6.3.1. До начала выполнения Работником Оператора своих должностных обязанностей, с ним должен быть проведен инструктаж в соответствии с требованиям нормативно-правовых актов РФ и организационно-распорядительной документации Оператора, в том числе настоящей Политики.

6.3.2. Для выполнения требований по Информационной безопасности Работники должны знать требования нормативно-правовых актов РФ и организационно-распорядительной документации Оператора.

6.4. Физическая защита.

6.4.1. Отдельные группы помещений, нахождение в которых посторонних лиц нежелательно (например, архивные помещения), могут отделяться дополнительными дверями, устройствами для опечатывания иными средствами ограничения доступа.

6.4.2. Работники Оператора не должны оставлять свои рабочие кабинеты без наблюдения. В случае если помещение остается без наблюдения, то оно должно быть закрыто на замок.

6.4.3. Работники сторонних организаций (обслуживающий персонал, осуществляющий сопровождение программного обеспечения или ремонт оборудования и т.д.) должны вызываться установленным порядком в случае необходимости. При приходе таких сотрудников без предварительной заявки их допуск в помещения Оператора должен осуществляться только по согласованию с ответственным лицом Оператора, в ведении которого предполагаются проводимые работы.

6.4.4. Проход посетителей или представителей сторонних организаций в помещения Оператора и контроль их нахождения в помещениях должен осуществляться в соответствии с порядком обеспечения пропускного режима здания, в котором располагаются указанные помещения.

6.5. Защита технических средств.

6.5.1. В соответствии с нормативными правовыми актами Российской Федерации, размещение монитором АРМ, обрабатывающих информацию ограниченного доступа, должно исключать возможность их просмотра лицами, не допущенными к данной информации.

6.5.2. При использовании систем видеонаблюдения, такие системы должны быть установлены в местах, исключающих просмотр содержимого мониторов АРМ, обрабатывающих информацию ограниченного доступа, а также исключающих просмотр вводимых паролей, кодов, шифров и т.д.

6.5.3. Документы, напечатанные на принтерах, должны быть изъяты из них.

6.5.4. Работникам запрещено подключать собственные технические средства, периферийные устройства, за исключением носителей информации, к АРМ и корпоративной сети без письменного согласования с руководством Оператора. Согласие руководства Оператора не требуется при осуществлении Работником трудовой функции в удаленном формате.

6.5.5. Все технические средства должны проходить техническое обслуживание. Такое обслуживание должно проводиться регулярно, но не реже сроков, указанных в эксплуатационной документации или организационно-распорядительных документах

Оператора. После окончания работ техническое средство опечатывается и возвращается на рабочее место.

6.5.6. Техническое устройства, необходимые для выполнения Работниками своих должностных обязанностей, рекомендуется оборудовать сетевыми фильтрами и/или источниками бесперебойного питания в целях предотвращения утечки информации по техническим каналам.

6.6. Парольная защита.

6.6.1. Доступ к программному обеспечению, за исключением 1С, используемому Работниками в рамках должностных обязанностей и подразумевающему наличие идентификации и аутентификации пользователя и/или разграничение полномочий, без использования пароля запрещен.

6.6.2. Защитные меры от несанкционированного доступа к Персональным данным должны обеспечивать сокрытие вводимых Работниками аутентификационных данных на АРМ.

6.6.3. Пароли доступа к различному прикладному программному обеспечению, используемому Работниками в рамках должностных обязанностей, должны отличаться от паролей доступа к АРМ или к ресурсам корпоративной сети и не должны совпадать для различного программного обеспечения.

6.6.4. В качестве паролей рекомендуется использовать пароли, представляющие собой комбинацию латинских букв (прописных и строчных) , цифр и специальных символов.

6.7. Антивирусная защита.

6.7.1. Антивирусное программное обеспечение должно быть установлено и функционировать в штатном режиме на всех серверах корпоративной сети, АРМ, как отдельно стоящих, так и подключенных к корпоративной сети, на портативных компьютерах.

6.7.2. Не допускается изменение настроек системы антивирусной защиты в части оповещения о нахождении компьютерных вирусов или вредоносных программ, в результате которого уменьшается эффективность работы данной системы.

6.7.3. Обновление баз системы антивирусной защиты должно производиться с регулярностью, обеспечивающей ее эффективное функционирование.

6.7.4. Запрещается отключение системы антивирусной защиты, за исключением случаев проведения тестирования программного обеспечения и иных тестов, проводимых уполномоченными Работниками Оператора.

6.7.5. Файлы, полученные любым образом, с любых носителей информации или сетей общего пользования должны быть проверены на наличие вредоносного кода.

6.7.6. Устанавливаемое или изменяемое программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

6.7.7. Должны быть определены, выполняться и контролироваться процедуры, выполняемые в случае обнаружения компьютерных вирусов, в которых, в частности, необходимо зафиксировать:

6.7.7.1. Необходимые меры по отражению и устранению последствий вирусной атаки;

6.7.7.2. Порядок официального информирования непосредственного руководителя;

6.7.7.3. Порядок приостановления при необходимости работы (на период устранения последствий вирусной атаки).

6.7.8. Подключение к АРМ незарегистрированных отчуждаемых носителей информации (дискеты, компакт-диски, съемные жесткие диски, мобильные телефоны, ноутбуки и иные носители информации) разрешено только с обязательной проверкой таких носителей на наличие компьютерных вирусов и/или вредоносных программ.

6.7.9. В случае получения файлов, проверка которых в исходном состоянии невозможна (например, файлы содержат архивы, неподдерживаемые системой антивирусной защиты, файлы прошли криптографическое преобразование и т.д.), необходимо на АРМ, не подключенном к корпоративной сети Оператора, привести данные файлы к состоянию пригодному для проверки на наличие вредоносного кода, осуществить такую проверку, после чего принимать решение о возможности использования данных файлов.

6.7.10. Любые намеренные попытки написания, компиляции, интерпретации, хранения, запуска или распространения пользователям компьютерных вирусов или вредоносных программ, а также иного кода, предназначенного для саморазмножения, нанесения ущерба или снижения производительности автоматизированных систем Оператора, запрещены.

6.8. Использование сети Интернет.

6.8.1. Ресурсы сети Интернет используются Оператором для получения информации, связанной с профессиональной деятельностью, информационно-аналитической работой, в том числе сбором статистических сведений. Иное использование ресурсов сети Интернет должно рассматриваться как нарушение Информационной безопасности.

6.8.2. В связи с повышенными рисками Информационной безопасности при взаимодействии с сетью Интернет должны применяться соответствующие средства защиты конфиденциальной информации, обеспечивающие прием и передачу информации только в установленном формате и только для конкретной определенной настоящей Политикой цели. Предназначенные для этого средства защиты информации, в том числе криптографические, должны пройти сертификацию в установленном законодательством Российской Федерации порядке.

6.8.3. Вся информация, полученная из сети Интернет, должна считаться недостоверной, не будучи подтвержденной из других источников.

6.8.4. Для получения возможности доступа пользователя в сеть Интернет необходимо использование технологий идентификации и аутентификации, а также должны быть обеспечены механизмы защиты информационных ресурсов Оператора от воздействия из сети Интернет.

6.8.5. Пользователям запрещено использование любых способов доступа в сеть Интернет (например, dial-up, использование доступа через операторов сотовой связи, 3G-модем и т.д.), отличных от установленных. В случаях, если необходимо осуществить доступ в сеть Интернет, отличный от установленных, то такой доступ должен быть согласован с руководством Оператора и лицом, ответственным за Информационную безопасность.

6.8.6. Передача информации ограниченного доступа по сети Интернет допускается при условии соблюдения всех требований к такой передаче, утвержденных у Оператора.

6.8.7. Пользователю запрещено любое тестирование и/или попытка обхода установленных механизмов защиты.

6.8.8. Запрещено предоставлять доступ в сеть Интернет стороннему обслуживающему персоналу и иным лицам, состоящим в договорных отношениях с Оператором, за исключением случаев, когда такой доступ необходим для исполнения договорных обязательств в интересах Оператора.

6.8.9. Получение доступа пользователя к ресурсам сети Интернет не означает, что пользователь имеет неограниченные возможности при работе с данным ресурсом. Запрещено получение из сети Интернет информации рекламного, порнографического и иного характера и использование для участия в игровых, развлекательных и иных ресурсах (включая конкурсы, выставки, социальные сети и иные Интернет-сообщества).

6.8.10. Работникам запрещена самостоятельная загрузка любого программного обеспечения из сети Интернет. В случаях, когда загрузка программного обеспечения продиктована выполнением функций и задач Оператора, загрузка программного обеспечения из сети Интернет осуществляется уполномоченными на это Работниками Оператора.

6.8.11. Работникам запрещено участвовать в обмене пиратским программным обеспечением, серийными номерами программного обеспечения и ином обмене, нарушающем и/или ущемляющем права правообладателей обмениваемой информации.

6.8.12. В случае получения сообщения о выявленной уязвимости пользователь обязан передать данное сообщение уполномоченному Работнику Оператора. Работнику запрещено предпринимать любые самостоятельные попытки устранения уязвимостей, кроме выполнения прямых указаний уполномоченного Работника Оператора и запрещено передавать информацию о выявленных или потенциальных угрозах уязвимости другим Работникам.

6.9. Использование электронной почты.

6.9.1. Все системы электронной почты должны быть использованы Работниками только для выполнения должностных обязанностей, выполнения договорных обязательств и выполнения требований нормативных правовых актов Российской Федерации.

6.9.2. Использование всех систем электронной почты должно осуществляться с применением технологий идентификации и аутентификации.

6.9.3.Запрещено использовать электронную почту для отправления писем, содержание которых может считаться незаконным, оскорбительным.

6.9.4. Запрещено использовать электронную почту с целью отправки сообщения с чужого почтового ящика или от чужого имени, отправки сообщений в личных или благотворительных целях, не связанных с деятельностью Оператора, отправки и пересылки писем, пересылаемых по цепочке, массовой рассылки писем, кроме случаев, когда необходимо оповещение большого числа Работников Оператора или в случаях, когда это обусловлено выполнением задач Оператора.

6.9.5. Пользователям запрещено открывать вложения в электронные сообщения, в случае если отправитель данного сообщения не известен пользователю. Открывать вложения от неизвестных сообщений разрешено только Администратору.

6.9.6. Пользователям запрещено отвечать на запросы любой персональной идентификационной информации, включая пароли, коды доступа, номера кредитных карт и т.д. В случае получения сообщений с такими запросами пользователь обязан сообщить о них Администратору.

6.10. Использование съемных носителей информации.

6.10.1. Работники, которым необходимо использование съемных носителей информации для выполнения должностных обязанностей, должны быть обеспечены такими носителями Оператором. Использование личных съемных носителей информации Работников для выполнения должностных обязанностей разрешено при условии выполнения требований настоящей Политики. Необходимость использования Работниками личных съемных носителей должна быть сведена к минимуму.

6.10.2. Использование личных съемных носителей должно соответствовать требованиям нормативных правовых актов Российской Федерации, а также локальных актов Оператора;

6.10.3. Эксплуатация съемных носителей информации должна осуществляться в соответствии с требованиями по их эксплуатации и быть направлена на предупреждение их неисправности.

6.10.4. Съемные носители должны храниться и утилизироваться надежно и безопасно. Если носители планируется использовать в пределах Оператора для другого прикладного программного обеспечения, информация на них должна быть уничтожена.

6.10.5. Подключение съемных носителей информации к техническим средствам, заведомо содержащим вирусы и/или вредоносное программное обеспечение, запрещено. В этом случае съемные носители передаются Администратору.

6.11. Использование мобильных устройств.

6.11.1. Под мобильным устройством понимается любое устройство обработки информации в электронном виде по особенностям своей конструкции для обработки информации без привязки к определенному месту (ноутбуки, планшеты, смартфоны и т.д.).

6.11.2. Использование сотрудниками личных мобильных устройств для выполнения должностных обязанностей запрещено, за исключением случаев совершения телефонных звонков по личным мобильным телефонам и использования рабочей электронной почты.

6.11.3. Служебные мобильные устройства должны отвечать требованиям настоящей Политики, включая требования по парольной защите, антивирусной защите, установленному программному обеспечению и т.д. Служебные мобильные устройства, не отвечающие требованиям настоящей Политики, запрещено использовать для выполнения должностных обязанностей сотрудниками, в том числе подключать их к корпоративной сети Оператора.

6.11.4. Обработка информации ограниченного доступа на мобильных устройствах должна соответствовать требованиям нормативных правовых актов Российской Федерации и локальных актов Оператора.

6.11.5. Работник, использующий служебные мобильные устройства, несет персональную ответственность за обеспечение их сохранности. Сотрудникам запрещено создавать предпосылки для осуществления утраты, кражи и иных противоправных действий со служебными мобильными устройствами.

6.11.6. Использование служебных мобильных устройств в личных целях, а также для совершения противоправных действий, запрещено.

6.12. Использование средств криптографической защиты.

6.12.1. Средства криптографической защиты информации (далее - СКЗИ) предназначены для защиты информации при ее обработке, хранении и передачи по каналам связи.

6.12.2. Применение СКЗИ должно проводиться в соответствии с моделью угроз и моделью нарушителя. Установка и настройка средств СКЗИ должна производиться только с дистрибутива, полученного по доверенному каналу. При установке программного обеспечения СКЗИ должен быть обеспечен контроль целостности и достоверность дистрибутива.

6.12.3. Деятельность с СКЗИ должна исключать нарушение законодательства Российской Федерации в области лицензирования. В случае, если предполагаемая деятельность с СКЗИ предполагает необходимость получения лицензии, то Оператор обязан получить такую лицензию или привлекать для подобной деятельности сторонние организации, имеющие соответствующие лицензии.

6.12.4. Для обеспечения безопасности необходимо использовать СКЗИ, которые:

6.12.4.1. Сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России.

6.12.4.2. Допускают встраивание в технологические процессы обработки электронных сообщений, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов.

6.12.5. Установка и ввод в эксплуатацию, а также эксплуатация средств криптографической защиты информации должны осуществляться в соответствии с эксплуатационной и технической документацией к этим средствам.

6.12.6. На технических средствах АРМ с установленным СКЗИ необходимо использовать только лицензионное программное обеспечение.

6.12.7. При использовании СКЗИ для защиты информации ограниченного доступа данные СКЗИ должны соответствовать требованиям законодательства Российской Федерации.

6.12.8. Установка, настройка и техническое обслуживание СКЗИ должно отвечать требованиям законодательства Российской Федерации.

6.12.9. Перед использованием СКЗИ Работники должны пройти обучение по порядку их использования.

6.12.10. Пользователям запрещено использование СКЗИ других пользователей, в том числе с целью выдать себя за другого пользователя.

6.12.11. Все действия по сохранности СКЗИ, в том числе их токенов, должны быть направлены на исключение их компрометации.

6.12.12. В случае компрометации ключей или подозрения на компрометацию пользователь обязан прекратить любое использование СКЗИ и незамедлительно сообщить о данном факте Администратору.

6.13. Резервное копирование.

6.13.1. Порядок резервного копирования распространяется только на рабочую информацию, хранящуюся на информационных ресурсах и в Базах данных Оператора.

6.13.2. Резервное копирование должно сочетать как минимум две технологии резервного копировании, одной из которых должна быть технология RAID, используемая для создания дисковых массивов на аппаратных ресурсах Оператора.

6.13.3. Регулярность создания резервных копий рабочей информации должна быть достаточной для продолжения нормальной работы Оператора, в случае нарушения целостности и/или доступности рабочей информации на информационных ресурсах Оператора, но не реже одного раза в день для ежедневно изменяющихся данных и одного раза в неделю для периодически изменяющихся данных. Копирование резервных копий на отчуждаемые носители

(внешние дисковые хранилища и т.п.) должно осуществляться регулярно, но реже одного раза в месяц.

6.13.4. Все резервные копии, должны быть размещены в отдельных каталогах, название которых отражает дату последнего изменения рабочей информации и ее краткое описание.

6.13.5. Вся рабочая информация, хранящаяся на аппаратных ресурсах Оператора и регулярно копируемая на отчуждаемые носители, должна быть доступна для дальнейшего восстановления.

6.13.6. Как минимум одна резервная копия рабочей информации должна храниться на съемном носителе.

6.13.7. Процессы резервного копирования и восстановления для каждого отдельного типа информации должны быть документированы и периодически пересматриваться.

6.13.8. Для хранения резервных копий на съемных носителях должны выбираться такие съемные носители, характеристики которых не изменяются в течение предполагаемого времени хранения резервных копий.

6.13.9. Резервные копии, хранящиеся более полугода, должны ежеквартально тестироваться, для подтверждения возможности их восстановления и использования.

6.14. Работа с электронной подписью.

6.14.1. Электронная подпись (далее - ЭП) выдается руководителю или иному уполномоченному должностному лицу Оператора и предназначена для использования в информационных системах, в которых электронные документы признаются эквивалентными их аналогам на бумажном носителе.

6.14.2. В случае компрометации закрытого ключа ЭП владелец сертификата немедленно извещает Администратора.

6.14.3. К событиям, связанным с компрометацией ключей, относятся следующие ситуации:

6.14.3.1. Утрата ключевых носителей.

6.14.3.2. Утрата ключевых носителей с их последующим обнаружением.

6.14.3.3. Нарушение правил хранения и уничтожения закрытого ключа.

6.14.3.4. Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи.

6.14.4. Выведенные из действия закрытые ключи ЭП подлежат уничтожению.

6.14.5. В целях обеспечения Информационной безопасности Работники, являющиеся владельцами сертификата ЭП, обязаны:

6.14.5.1. Хранить в тайне закрытый ключ ЭП.

6.14.5.2. Немедленно требовать приостановления действия с последующим аннулированием сертификата, если тайна закрытого ключа ЭП нарушена.

6.14.5.3. Участвовать в плановой смене сертификатов ключей подписи.

6.14.6. Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

6.14.7. Запрещается:

6.14.7.1. Снимать несанкционированные Администратором копии с ключевых носителей.

6.14.7.2. Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей (монитор) АРМ или принтер.

6.14.7.3. Устанавливать ключевой носитель в считывающее устройство АРМ в режимах, не предусмотренных функционированием системы, а также устанавливать носитель в другие АРМ.

6.14.7.4. Записывать на ключевой носитель постороннюю информацию.

6.14.7.5. Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

VII. Модель угроз

7.1. Целью определения угроз Информационной безопасности является установление возможного нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной Системе Оператора, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора, а в случае обработки Персональных данных и для Субъектов.

7.2. Определение угроз безопасности должно носить систематический характер и осуществляться как на этапе создания элементов информационной системы Оператора и формирования требований по их защите, так и в ходе их эксплуатации. Систематический подход к определению угроз безопасности информации необходим для того, чтобы определить потребности в конкретных требованиях к защите информации и создать адекватную эффективную систему защиты информации в информационной системе. Меры защиты информации, принимаемые Оператором, должны обеспечивать эффективное и своевременное выявление и блокирование (нейтрализацию) угроз безопасности информации, в результате реализации которых возможно наступление неприемлемых негативных последствий (ущерба).

7.3. Угрозы безопасности информации характеризуются источниками угроз, способами (методами) реализации угроз и последствиями от реализации угроз безопасности информации.

7.4. В качестве источников угроз безопасности информации могут выступать как субъекты (физические лица, юридические лица) или явления (природные или техногенные).

7.5. Источники угроз безопасности являются определяющим фактором при определении угроз безопасности информации.

7.6. Источники угроз безопасности могут быть следующих типов:

7.6.1. Неблагоприятные события техногенного характера:

7.6.2. Сбои и отказы в работе объектов и (или) ресурсов доступа;

7.6.3. Зависимость процессов эксплуатации объектов информатизации от иностранных поставщиков и провайдеров услуг;

7.6.4. Внутренние нарушители безопасности информации – лица, в том числе Работники, реализующие угрозы безопасности информации с использованием легально предоставленных им прав логического и физического доступа;

7.6.5. Внешние нарушители безопасности информации – лица, в том числе Работники, реализующие угрозы безопасности информации без использования легально предоставленных прав логического или физического доступа, а также субъекты, не являющиеся Работниками, реализующие целенаправленные компьютерные атаки, в том числе с целью личного обогащения или блокирования штатного функционирования бизнес-процессов или технологических процессов Оператора

7.7. Пересмотр угроз безопасности информации, как минимум, осуществляется в следующих случаях:

7.7.1. Изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регламентирующих защиту информации.

7.7.2. Изменения конфигурации (состава основных компонентов) и особенностей функционирования информационной системы, следствием которых стало возникновение новых угроз информационной безопасности информации.

7.7.3. Выявление уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих угроз.

7.7.4. Появление сведений и фактов о новых возможных нарушителях безопасности информации.

7.8. Приведенные в настоящем разделе Политики модели угроз с учетом следующих уровней информационной инфраструктуры:

7.8.1. Системные уровни:

7.8.1.1. уровень аппаратного обеспечения;

7.8.1.2. уровень сетевого оборудования;

7.8.1.3. уровень сетевых приложений и сервисов;

7.8.1.4. уровень серверных компонентов виртуализации, программных инфраструктурных сервисов;

7.8.1.5. уровень операционных систем, систем управления базами данных, серверов приложений.

7.8.2. Уровень АС и приложений, эксплуатируемых для оказания финансовых услуг в рамках бизнес-процессов или технологических процессов Оператора.

7.9. К числу наиболее актуальных источников угроз на уровне аппаратного обеспечения, уровне сетевого оборудования и уровне сетевых приложений и сервисов относятся следующие:

7.9.1. сбои и отказы в работе объектов доступа;

7.9.2. внутренние нарушители безопасности информации (эксплуатационный, вспомогательный (технический) персонал), осуществляющие целенаправленное деструктивное воздействие на объекты доступа;

7.9.3. зависимость процессов эксплуатации объектов доступа от иностранных поставщиков или провайдеров услуг;

7.9.4. внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;

7.9.5. внешние нарушители безопасности информации, организующие DoS, DdoS и иные виды компьютерных атак;

7.9.6. комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие совместно и (или) согласованно.

7.10. К числу наиболее актуальных источников угроз на уровне серверных компонентов виртуализации, программных инфраструктурных сервисов, операционных систем, систем управления базами данных и серверов приложений относятся следующие:

7.10.1. внутренние нарушители безопасности информации (эксплуатационный персонал), осуществляющие целенаправленные деструктивные воздействия на ресурсы доступа;

7.10.2. внутренние нарушители безопасности информации (эксплуатационный персонал), реализующие угрозы безопасности информации с использованием легально предоставленных прав логического доступа;

7.10.3. сбои и отказы в работе ПО;

7.10.4. зависимость процессов эксплуатации ресурсов доступа, ПО от иностранных поставщиков или провайдеров услуг;

7.10.5. внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;

7.10.6. комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие в сговоре.

7.11. К числу наиболее актуальных источников угроз на уровне АС и приложений, эксплуатируемых в рамках бизнес-процессов и технологических процессов Оператора, относятся следующие:

7.11.1. внутренние нарушители безопасности информации (пользователи и эксплуатационный персонал АС и приложений), реализующие угрозы безопасности с использованием легально предоставленных прав логического доступа;

7.11.2. внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;

7.11.3. зависимость процессов эксплуатации АС и приложений от иностранных поставщиков или провайдеров услуг;

7.11.4. комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие в сговоре.

VIII Модель нарушителя

8.1. Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе Оператора с

заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциалом этих нарушителей и возможных способах реализации угроз безопасности информации.

8.2. Результаты оценки возможностей нарушителей включаются в модель нарушителя, которая является составной частью (разделом) модели угроз безопасности информации и содержит:

8.2.1. Типы нарушителей, которые могут обеспечить реализацию угроз безопасности информации.

8.2.1.1. Типы нарушителей определяются по результатам анализа прав доступа Субъектов к информации, а также анализа возможностей нарушителей по доступу к компонентам информационной системы, исходя из структурно-функциональных характеристик и особенностей функционирования информационной системы.

8.2.1.2. Анализ прав доступа проводится, как минимум, в отношении следующих компонентов информационной системы:

- устройства ввода/вывода информации;
- беспроводных устройств;
- программных, программно-технических и технических средств обработки информации;
- съемных машинных носителей информации;
- машинных носителей информации, выведенных из эксплуатации;
- активного (коммутационного) и пассивного оборудования каналов связи;
- каналов связи, выходящих за пределы контролируемой зоны.

8.2.1.3. С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

- внешние нарушители – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;
- внутренние нарушители – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

8.2.1.4. Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. При оценке возможностей внутренних нарушителей необходимо учитывать принимаемые Оператором организационные меры по допуску Субъектов к работе в информационной системе. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка доступа физических лиц к информационной системе и ее компонентам, а также мер по контролю за доступом и работой этих лиц.

8.2.1.5. Внешнего нарушителя необходимо рассматривать в качестве актуального во всех случаях, когда имеются подключения информационной системы к внешним информационно-телекоммуникационным сетям, в том числе к сети Интернет, и (или) имеются связи, выходящие за пределы контролируемой зоны, используемые для иных подключений.

8.2.2. Виды нарушителей.

8.2.2.1. Угрозы безопасности информации в информационной системе Оператора могут быть реализованы следующими видами нарушителей:

- специальные службы иностранных государств;
- террористические, экстремистские группировки;
- преступные группы (криминальные структуры);
- внешние субъекты (физические лица и юридические лица);
- разработчики, производители, поставщики программных, технических и программно-технических средств;
- лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;
- лица, обеспечивающие функционирование информационной системы

8.2.2.2. Виды нарушителей определяются на основе предположений (прогноза) о возможных целях (мотивации) при реализации угроз безопасности информации этими нарушителями.

8.2.2.3. В качестве возможных целей (мотивации) реализации нарушителями угроз безопасности информации в информационной системе могут быть:

- нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;
- реализация угроз безопасности информации по идеологическим или политическим мотивам;
- организация террористического акта;
- причинение имущественного ущерба путем мошенничества или иным преступным путем;
- дискредитация или дестабилизация деятельности органов государственной власти, организаций;
- получение конкурентных преимуществ;
- внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;
- любопытство или желание самореализации;
- выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;
- реализация угроз безопасности информации из мести;
- реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий.

8.2.2.4. Предположения о целях (мотивации) нарушителей делаются с учетом целей и задач информационной системы, вида обрабатываемой информации, а также с учетом результатов оценки степени возможных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации.

8.2.2.5. Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

8.2.2.6. В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

- нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в ИС;
- нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в ИС;
- нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в ИС.

8.2.3. Потенциал нарушителей.

8.2.3.1. Целью определения возможных способов реализации угроз безопасности информации является формирование предположений о возможных сценариях реализации угроз безопасности информации, описывающих последовательность (алгоритмы) действий отдельных видов нарушителей или групп нарушителей и применяемые ими методы и средства для реализации угроз безопасности информации.

8.2.3.2. Возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования ИС.

8.2.3.3. Угрозы безопасности информации могут быть реализованы нарушителями за счет:

- несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы, установленные в аппаратных компонентах, чипсетах);
- несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);

- несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, иные прикладные программы общего и специального назначения);

- несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

- несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;

- воздействия на пользователей, администраторов безопасности, ответственных за объекты информатизации или обслуживающий персонал (социальная инженерия).

IX. Права и обязанности сторон в области обработки Персональных данных

9.1. Субъект Персональных данных обязан предоставлять Оператору достоверные сведения о себе.

Оператор оставляет за собой право проверять достоверность сведений, сверяя данные, предоставленные Субъектом Персональных данных, с имеющимися документами.

Субъект Персональных данных обязан воздерживаться от разглашения Персональных данных других Субъектов Персональных данных.

Субъекты Персональных данных обязаны использовать Персональные данные других Субъектов Персональных данных лишь в целях, для которых они были сообщены.

9.2. В случае если на основании Персональных данных Субъекта Персональных данных невозможно достоверно установить какие-либо обстоятельства, учет которых необходим при принятии решений, затрагивающих права Субъекта Персональных данных в рамках трудовых отношений, Работодатель может предложить Субъекту Персональных данных представить разъяснения и уточнения в отношении своих Персональных данных в любой удобной форме.

9.3. При изменении Персональных данных, содержащихся в документах, указанных в пункте 1.5 Политики (включая фамилию, имя, отчество, адрес фактического места жительства, паспортные данные, сведения о состоянии здоровья (вследствие выявленных в соответствии с медицинским заключением противопоказаний для выполнения Субъектом Персональных данных его должностных обязанностей) и др.), если инициатором таких изменений не является сам Работодатель, Субъект Персональных данных обязан письменно уведомить Работодателя о таких изменениях в срок, не превышающий 3х (трех) рабочих дней.

9.4. По мере необходимости Работодатель может истребовать у Субъекта Персональных данных дополнительные Персональные данные. Если обязанность предоставления Персональных данных для Субъекта Персональных данных установлена действующим законодательством, Оператор обязан разъяснить Субъекту Персональных данных юридические последствия отказа предоставить свои Персональные данные.

9.5. В целях обеспечения защиты Персональных данных, хранящихся у Оператора, Субъекты Персональных данных имеют право:

- получать полную информацию о своих Персональных данных.
- получать информацию, касающуюся обработки своих Персональных данных, включая: подтверждение факта обработки Персональных данных Оператором, а также цель такой обработки; способы обработки Персональных данных, применяемые Оператором; сведения о лицах, которые имеют доступ к Персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых Персональных данных и источник их получения; сроки обработки Персональных данных, в том числе сроки их хранения.
- свободного бесплатного доступа к своим Персональным данным.

9.6. Оператор, как обладатель информации, информационной системы, включающей в себя Персональные данные Субъекта Персональных данных, в случаях, установленных законодательством Российской Федерации, обязан обеспечить:

- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий в результате нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

9.7. Оператор обязан предупредить лиц, получающих Персональные данные Субъекта Персональных данных, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено (в форме обязательства о неразглашении). Лица, получающие Персональные данные Субъекта Персональных данных, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен Персональными данными Субъектов Персональных данных в порядке, установленном федеральными законами Российской Федерации.

X. Разграничение прав доступа к Персональным данным

10.1. Разграничение прав осуществляется исходя из категории Субъектов Персональных данных (в зависимости от того, обрабатываются Персональные данные Работника как Субъекта Персональных данных или иного лица как Субъекта Персональных данных), характера и режима обработки Персональных данных в информационной системе Персональных данных (ИСПДн).

10.2. Список групп должностных лиц, ответственных за обработку Персональных данных Работников как Субъектов Персональных данных в ИСПДн, а также их уровень прав доступа в ИСПДн представлен в Приложении №6 к данной Политики.

10.3. Список групп должностных лиц, ответственных за обработку Персональных данных Субъектов Персональных данных, не являющихся Работниками в ИСПДн, а также их уровень прав доступа в ИСПДн представлен в Приложении №6.1 к данной Политики.

10.4. При внесении изменений в Приложения № 6, 6.1, 7, 7.1 к настоящей Политики, новые редакции указанных Приложений подлежат утверждению приказом руководителя Оператора.

10.5. Основные группы пользователей ИСПД

- Администраторы ИСПДн – осуществляют настройку и установку технических средств ИСПДн и обеспечивают ее бесперебойную работу;
- Пользователи ИСПДнс правами записи – осуществляют текущую работу с Персональными данными со всеми правами по обработке Персональных данных;
- Пользователи ИСПДн без права записи — осуществляют текущую работу с Персональными данными с правом чтения Персональных данных.

10.6. Распределение уровня доступа к Персональным данным:

Группа	**Уровень доступа к ПД**	**Разрешенные действия**
Администратор ИСПДн (Администратор)	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн, в том числе о системном и прикладном программном обеспечении ИСПДн, о технических средствах и конфигурации	Защита Персональных данных.

	ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Располагает всей информацией о топологии ИСПДн и технических средствах обработки и защиты Персональных данных, обрабатываемых в ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	
Пользователи с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем Персональным данным.	Сбор, систематизация, накопление, хранение, уточнение, использование Уничтожение Персональных данных.
Пользователи без права записи	Обладают только правом чтения Персональных данных.	Чтение.

10.7. При увольнении или изменении должностных обязанностей Работников, имевших доступ к Персональным данным, необходимо выполнить регламентированные процедуры соответствующего пересмотра прав доступа.

10.8. Работники, имеющие доступ к Персональным данным, до начала работы с Персональными данными обязуются ознакомиться с настоящей Политикой.

XI. Ответственность за разглашение конфиденциальной информации, связанной с Персональными данными Субъекта Персональных данных

11.1. Информация, относящаяся к Персональным данным Субъекта Персональных данных, является конфиденциальной и охраняется законодательством Российской Федерации.

XI. Заключительные положения

12.1. Контроль за исполнением настоящей Политики возлагается на Генерального директора Общества.

12.2. При приеме на работу к Работодателю лицо, поступающее на работу, до подписания трудового договора, должно быть в обязательном порядке ознакомлено с настоящей Политикой, что подтверждается подписью лица в листе ознакомления с настоящими правилами, являющимся неотъемлемой частью настоящей Политики.

ПРИЛОЖЕНИЕ № 1
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

РАБОТНИКА АО СГ «Спасские ворота»

Я, _____
(Ф.И.О.)

Адрес места жительства: _____
_____
_____

Паспорт _____ Выдан «____» _____ _____г.

Кем выдан _____
_____

Настоящим я представляю Работодателю **АО СГ «Спасские ворота»** (ОГРН 1028900507668 , ИНН 8901010104), зарегистрированному по адресу: **г. Москва, ул. Ибрагимова, дом 15, корп. 2,** свои персональные данные в целях обеспечения соблюдения трудового законодательства и иных нормативно-правовых актов при содействии в трудоустройстве, обучении и продвижении по работе, обеспечения личной моей безопасности, текущей трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Моими персональными данными является любая информация, относящаяся ко мне как к физическому лицу (субъекту персональных данных), указанная в трудовом договоре, личной карточке работника (унифицированная форма Т-2) трудовой книжке и (или) сведениях о трудовой деятельности и полученная в течение срока действия настоящего трудового договора, в том числе:

- моя фамилия, имя, отчество;
- год, месяц, дата и место рождения;
-гражданство;
-документы, удостоверяющие личность;
-идентификационный номер налогоплательщика;
-страховой номер индивидуального лицевого счета;
- адреса фактического места проживания и регистрации по местожительству;
-почтовые и электронные адреса;
- номера телефонов,
- фотографии,
- сведения об образовании, профессии, специальности и квалификации,
- семейном положении и составе семьи,
- сведения об имущественном положении,
-доходах, задолженности,
- занимаемых ранее должностях и стаже работы,
- социальных льготах;
- воинском учете;
-сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной

переподготовке, поощрениях и наказаниях, видах и периодах отпуска, временной нетрудоспособности, командировании, рабочем времени и пр.);
- о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора.
- заявления, объяснительные и служебные записки;
- наличие судимостей;
- медицинские заключения, предъявляемые при прохождении обязательных предварительных и периодических медицинских осмотров.

Своей волей и в своих интересах выражаю согласие на осуществление Работодателем (оператором) любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных целей, в том числе выражаю согласие на обработку без ограничения моих персональных данных, включая:
- сбор,
- систематизацию, накопление,
- хранение, уточнение (обновление, изменение),
- использование,
- предоставление,
- доступ,
- обезличивание,
- блокирование,
- уничтожение персональных данных при автоматизированной и без использования средств автоматизации обработке;
- запись на электронные носители и их хранение;
- передачу Работодателем (оператором) по своему усмотрению данных и соответствующих документов, содержащих персональные данные, третьим лицам: налоговым органам, в отделения Пенсионного фонда, Фонда социального страхования, Фонда обязательного медицинского страхования, правоохранительные органы; в военкомат; банкам в рамках перечисления заработной платы и прочих выплат; подразделения муниципальных органов управления, органы статистики.
- хранение моих персональных данных в течение 75 лет, если они закончены делопроизводством до 1 января 2003 года, если указанные документы закончены делопроизводством после 1 января 2003 года, то в течение 50 лет,

а также при осуществлении любых иных действий с моими персональными данными, указанными в трудовом договоре и полученными в течение срока действия трудового договора, в соответствии с требованиями действующего законодательства РФ и Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Работодателю (оператору) заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать Работодателю (оператору) об изменении местожительства, контактных телефонов, паспортных, документных и иных персональных данных в срок 5 рабочих дней.
Об ответственности за достоверность представленных персональных сведений предупрежден(а).

_____ _____
(подпись) (фамилия, имя)

«_____» _____ 20 _____ г.

ПРИЛОЖЕНИЕ № 1.1
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

АО СГ «Спасские ворота»

Я, _____

(Ф.И.О.)

Адрес места жительства: _____

_____

_____

Паспорт _____ Выдан «____» _____ _____г.

Кем выдан _____

_____

Настоящим я представляю Оператору **АО СГ «Спасские ворота»** (ОГРН 1028900507668 , ИНН 8901010104), зарегистрированному по адресу: **г. Москва, ул. Ибрагимова, дом 15, корп. 2,** свои персональные данные в целях обеспечения соблюдения договорных отношений и иных нормативно-правовых актов при исполнение договорных и иных обязательств.

Моими персональными данными является любая информация, относящаяся ко мне как к субъекту персональных данных, в том числе:

- моя фамилия, имя, отчество;
- год, месяц, дата и место рождения;
-гражданство;
-документы, удостоверяющие личность;
-идентификационный номер налогоплательщика;
-страховой номер индивидуального лицевого счета;
- адреса фактического места проживания и регистрации по местожительству;
-почтовые и электронные адреса;
- номера телефонов,
- фотографии,
- сведения об образовании, профессии, специальности и квалификации,
- наличие судимостей;

Своей волей и в своих интересах выражаю согласие на осуществление Оператором любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных целей, в том числе выражаю согласие на обработку без ограничения моих персональных данных, включая:

- сбор,
- систематизацию, накопление,
- хранение, уточнение (обновление, изменение),
- использование,
- предоставление,
- доступ,
- обезличивание,
- блокирование,

- уничтожение персональных данных при автоматизированной и без использования средств автоматизации обработке;
- запись на электронные носители и их хранение;
- передачу Оператором по своему усмотрению данных и соответствующих документов, содержащих персональные данные, третьим лицам: налоговым органам, в правоохранительные органы; банкам в рамках перечисления и получения денежных средств по заключенным договорам; подразделения муниципальных органов управления, органы статистики.
- хранение моих персональных данных в течение 75 лет, если они закончены делопроизводством до 1 января 2003 года, если указанные документы закончены делопроизводством после 1 января 2003 года, то в течение 50 лет,

а также при осуществлении любых иных действий с моими персональными данными в соответствии с требованиями действующего законодательства РФ и Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Оператору заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать Оператору об изменении местожительства, контактных телефонов, паспортных, документных и иных персональных данных в срок 5 рабочих дней.

Об ответственности за достоверность представленных персональных сведений предупрежден(а).

_____ _____

(подпись) (фамилия, имя)

«_____» _____ 20 _____ г.

ПРИЛОЖЕНИЕ № 1.2
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

СОГЛАСИЕ НА РАСКРЫТИЕ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

АО СГ «Спасские ворота»

Я, _____
(Ф.И.О.)

Адрес места жительства: _____
_____
_____

Паспорт _____ Выдан «____» _____ _____г.

Кем выдан _____
_____

Настоящим я представляю Оператору **АО СГ «Спасские ворота»** (ОГРН 1028900507668 , ИНН 8901010104), зарегистрированному по адресу: **г. Москва, ул. Ибрагимова, дом 15, корп. 2,** свои биометрические персональные данные в целях раскрытия моих биометрических персональных данных, а именно:

- размещение моей фотографии на информационном стенде АО СГ «Спасские ворота» по адресу: **г. Москва, ул. Ибрагимова, дом 15, корп. 2.**

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Оператору заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать Оператору об изменении местожительства, контактных телефонов, паспортных, документных и иных персональных данных в срок 5 рабочих дней.

Об ответственности за достоверность представленных персональных сведений предупрежден(а).

_____ _____
(подпись) (фамилия, имя)

«_____» _____ 20 _____ г.

ПРИЛОЖЕНИЕ № 1.3
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

СОГЛАСИЕ НА ПЕРЕДАЧУ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬЕЙ СТОРОНЕ

АО СГ «Спасские ворота»

Я, _____
(Ф.И.О.)

Адрес места жительства: _____
_____
_____

Паспорт _____ Выдан «____» _____ _____г.

Кем выдан _____
_____

Настоящим я даю согласие Оператору **АО СГ «Спасские ворота»** (ОГРН 1028900507668 , ИНН 8901010104), зарегистрированному по адресу: **г. Москва, ул. Ибрагимова, дом 15, корп. 2,** на передачу своих персональных данных третьей стороне – ООО «_____» (_____) для _____:

Передаче подлежат следующие мои персональные данные:
- дата приема на работу;
- должность, по которой я выполняю трудовые обязанности;
- размер моей заработной платы.

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Оператору заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать Оператору об изменении местожительства, контактных телефонов, паспортных, документных и иных персональных данных в срок 5 рабочих дней.
Об ответственности за достоверность представленных персональных сведений предупрежден(а).

_____ _____
(подпись) (фамилия, имя)

«_____» _____ 20 _____ г.

ПРИЛОЖЕНИЕ № 2
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

Генеральному директору
АО СГ «Спасские ворота»

_____

от _____
Фамилия имя, отчество

ОТЗЫВ СОГЛАСИЯ
на обработку персональных данных

Я, _____,
Паспорт _____ № _____, выданный «____»_____ года
_____
_____
зарегистрированная(ый) по адресу: _____
_____
_____
в соответствии с п.1 ст.9 Федерального закона от 27 июля 2006 года № 152ФЗ «О персональных данных» отзываю у **АО СГ «Спасские ворота»** (ОГРН 1028900507668 , ИНН 8901010104), зарегистрированному по адресу: **г. Москва, ул. Ибрагимова, дом 15, корп. 2,** согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в течение трёх рабочих дней с момента поступления настоящего отзыва.

«_____»_____20_____

_____
(фамилия полностью, инициалы, подпись)

ПРИЛОЖЕНИЕ № 3
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

Работнику:
АО СГ «Спасские ворота»

_____
должность
_____
Фамилия, имя, отчество

УВЕДОМЛЕНИЕ
«_____»_____20___ № _____
о получении персональных данных от третьей стороны

Уважаемый _____!
имя, отчество работника

Уведомляем Вас о том, что Акционерным обществом Страховая группа «Спасские ворота» будут запрошены от третьей стороны_____
_____
указать название организации третьего лица и др.
следующие ваши персональные данные:
_____
перечисление персональных данных
_____
перечисление персональных данных
- _____
перечисление персональных данных
- _____
перечисление персональных данных
Данные сведения будут запрошены в целях/в связи с _____
_____
указать цель, причину получения персональных данных от 3-й стороны
Сведения будут запрашиваться в письменной форме при помощи/с помощью_____
_____
указать способ получения персональных данных от 3-й стороны: средств почтовой связи, факса, электронной почты, др.

Просим Вас дать согласие на получение персональных данных от третьей стороны в соответствии с пунктом 3 статьи 86 Трудового Кодекса Российской Федерации.

_____ И.О.Фамилия
должность (менеджер по персоналу/генеральный директор)

С уведомлением ознакомлен(а): «_____»_____20_____
_____
(фамилия полностью, инициалы, подпись)

ПРИЛОЖЕНИЕ № 4
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

Генеральному директору
АО СГ «Спасские ворота»
_____

от _____
_____
Фамилия, имя, отчество

СОГЛАСИЕ
на получение работодателем персональных данных от третьей стороны

Я, _____,
Паспорт _____ № _____, выданный «____»_____ года
_____
_____
зарегистрированная(ый) по адресу: _____
_____
_____
в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» даю согласие Акционерному обществу Страховая группа «Спасские ворота» (АО СГ «Спасские ворота»), расположенному по адресу: 105318, г. Москва, ул. Ибрагимова, д. 15, к. 2, на получение моих персональных данных:
- _____
перечисление персональных данных
- _____
перечисление персональных данных
- _____
перечисление персональных данных
- _____
перечисление персональных данных
от третьей стороны: _____
_____
указать название организации третьей стороны и др.

Настоящее Согласие действует со дня его подписания до дня отзыва в письменной форме.

«_____»_____20_____

_____
(фамилия полностью, инициалы, подпись)

ПРИЛОЖЕНИЕ № 5
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

Обязательство
о неразглашении персональных данных

Я, _____,
Паспорт_____ № _____, выданный «____»_____ года
_____
_____
понимаю, что получаю доступ к персональным данным работников и иных субъектов персональных данных АО СГ «Спасские ворота». Я также понимаю, что во время исполнения своих обязанностей в должности
_____, мне
приходится заниматься сбором, обработкой и хранением персональных данных указанных выше лиц.
Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в Политике в отношении сбора, обработки, защиты персональных данных и информационной безопасности в АО СГ «Спасские ворота».
Я подтверждаю, что не имею права разглашать сведения о (об):

- паспортных данных;
- трудовом и общем стаже;
- образовании, квалификации, специальности;
- воинском учете;
- наличии судимостей;
- социальных льготах;
- инвалидности;
- беременности женщины;
- донорстве;
- необходимости ухода за больным членом семьи;
- доходах с предыдущего места работы;
- анкетных и биографических данных;
- адресе места жительства, домашнем телефоне;
- составе семьи;
- месте работы или учебы членов семьи и родственников, их возрасте и образовании;
- характере взаимоотношений в семье;
- содержании трудового договора;
- занимаемой должности;
- заработной плате;
- наличии материальных ценностей;
- делах, содержащих материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- дела о служебных расследованиях;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей и т.п.;
- листках нетрудоспособности;
- табелях учета рабочего времени;
- содержании заключенных договоров;
- исполнении обязанностей и реализации прав, предусмотренных заключенными договорами;
- материалах выплатного дела по заключенным договорам страхования;
- актов о страховом случае.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных субъектов персональных данных, или их утраты я несу ответственность в соответствии со ст. 90

Трудового Кодекса РФ: привлечение к дисциплинарной и материальной ответственности, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

С Политикой в отношении сбора, обработки, защиты персональных данных в АО СГ «Спасские ворота» и гарантиях их защиты ознакомлен(а). «_____»_____20_____

_____

(фамилия полностью, инициалы, подпись)

ПРИЛОЖЕНИЕ № 6
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

Перечень лиц, получивших доступ к персональным данным Работников:

№№		Роль	ФИО	Степень доступа

ПРИЛОЖЕНИЕ № 6.1
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

Перечень лиц, получивших доступ к персональным данным Субъектов, не являющихся Работниками

№№		Роль	ФИО	Степень доступа

ПРИЛОЖЕНИЕ № 7.1
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

Перечень мест хранения материальных носителей персональных данных иных лиц, обрабатываемых без использования средств автоматизации

№№	Персональные данные	Место хранения
1	…	
2		
3		
4		

ПРИЛОЖЕНИЕ № 8
к Политике
в отношении сбора, обработки
защиты персональных данных
в АО СГ «Спасские ворота»

Обязательство о соблюдении режима конфиденциальности персональных данных работника

Я, _____,
(фамилия, имя, отчество)
работая в АО СГ «Спасские ворота» на должности _____
_____
_____
_____

ОБЯЗУЮСЬ:

1. Не разглашать, не раскрывать публично, а также соблюдать установленный Политикой порядок передачи третьим лицам сведений, составляющих персональные данные работников, которые мне будут доверены или станут известны по работе.

2. Выполнять относящиеся ко мне требования Политики, приказов, распоряжений, инструкций и других локальных нормативных актов по обеспечению конфиденциальности персональных данных и соблюдать правила их обработки.

3. В случае попытки посторонних лиц получить от меня сведения, составляющие персональные данные, немедленно сообщить руководителю структурного подразделения и начальнику отдела кадров.

4. В случае моего увольнения, все носители, содержащие персональные данные работников и иных субъектов персональных данных (документы, копии документов, дискеты, диски, магнитные ленты, распечатки на принтерах, черновики, кино- и фотонегативы, позитивы и пр.), которые находились в моем распоряжении, в связи с выполнением мною трудовых обязанностей, передать руководителю структурного подразделения или другому сотруднику по указанию руководителя структурного подразделения.

5. Сообщать руководителю структурного подразделения и начальнику отдела кадров об утрате или недостаче документов или иных носителей, содержащих персональные данные работников и иных субъектов персональных данных (удостоверений, пропусков и т.п.); ключей от хранилищ, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению персональных данных работников и иных субъектов персональных данных, а также о причинах и условиях возможной утечки сведений.

Мне известно, что нарушение мною обязанностей по обработке и защите персональных данных работников может повлечь дисциплинарную, административную, гражданско-правовую, уголовную ответственность в соответствии с федеральными законами.

"____" _____20___г.

_____
(подпись) (Ф.И.О. работника)

Прошнуровано,
пронумеровано и
скреплено печатью
22 (Двадцать два)
листа

Генеральный директор
Акционерного общества Страховая
группа «Спасские ворота»

Климов Дмитрий Валерьевич