« УТВЕРЖДЕНО»
Генеральный директор
АО «ФинИст»

Приказ № 21
от « 30» октября 2015 г.

ПОЛИТИКА
обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных АО «ФинИст»

1. ОБЩИЕ ПОЛОЖЕНИЯ.

Настоящая Политика устанавливает порядок отношений, связанных с обработкой персональных данных, осуществляемой Обществом с использованием средств автоматизации, в том числе информационно - телекоммуникационных сетях.

1.1 Цель

Целью настоящей Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе, защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2 Основания

Основанием для разработки данной Политики являются:

- Конституция Российской Федерации от 12.12.1993;
- Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 17.11.2007 г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Трудовой кодекс Российской Федерации от 30.12.2001г. №197-ФЗ;
- Кодекс Российской Федерации об административных правонарушениях от 30.12 2001 г. №195-ФЗ;
- Приказ ФСТЭК России от 05.02.2010 г. №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;
- Стандарт Науфор от 27.12.2010 г. «Обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных операторами – профессиональными участниками рынка ценных бумаг».

1.3. Порядок ввода в действие Политики обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Обществом (далее Политика)

Политика и изменения к ней вводятся приказом по Обществу, и утверждается Генеральным директором. Все сотрудники Общества должны быть ознакомлены под роспись с данной Политикой.

2. ОСНОВНЫЕ ПОНЯТИЯ, ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ.

- В целях настоящего Политики используются следующие основные понятия:
- **персональные данные** - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);
- **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Под персональными данными сотрудников и клиентов Общества понимается информация необходимая Обществу в связи с осуществлением трудовых и договорных отношений с конкретным сотрудником или клиентом, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника или клиента, позволяющие идентифицировать их личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

К персональным данным относятся:

- все биографические сведения сотрудника или клиента;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес местожительства;
- домашний телефон ;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т- 2) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета сотрудника;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным сотрудника.
- содержание договора, заключенного между Обществом и клиентом;
- документы, переданные клиентом при заключении договора.

Указанные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится.

Режим конфиденциальности персональных данных сотрудников снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

Режим конфиденциальности персональных данных клиентов снимается в случаях обезличивания, если иное не определено законом.

Собственником информационных ресурсов (персональных данных) является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил,/изъявил желание вступить в трудовые или договорные отношения с Обществом. Субъект персональных данных самостоятельно решает вопрос передачи Обществу своих персональных данных.

Держателем персональных данных является Общество, которому субъект персональных данных добровольно передает во владение свои персональные данные. Общество выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

Обработка персональных данных должна осуществляться на законной и справедливой основе.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Общество должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством РФ, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством РФ.

Обработка персональных данных включает в себя их сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных.

Все персональные данные сотрудника или клиента Общества получают у субъекта персональных данных. Если персональные данные, возможно, получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, если иное не предусмотрено законодательством РФ.

Не допускается получение и обработка персональных данных сотрудников и клиентов Общества об их расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

Субъект персональных данных обязан:

- передавать Обществу комплект достоверных, документированных персональных данных;
- своевременно сообщать Обществу об изменении своих персональных данных.

Субъект персональных данных имеет право:

- получать информацию, касающуюся обработки своих персональных данных;
- иметь доступ к своим персональным данным, за исключением случаев, предусмотренных законодательством РФ;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- принимать предусмотренные законодательством РФ меры по защите своих прав;
- определять представителей для защиты своих персональных данных;
- обжаловать действия или бездействия Общества в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке

4. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ.

Внешний доступ.

К числу массовых потребителей персональных данных вне Общества можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

Внутренний доступ.

Внутри Общества к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- сотрудники бухгалтерии;
- руководители Общества;
- специалисты Общества.

Доступ сотрудников Общества к персональным данным осуществляется исключительно для выполнения ими своих должностных обязанностей.

Сотрудники Общества, осуществляющие обработку персональных данных, должны быть ознакомлены с требованиями по обеспечению безопасности персональных данных в части, касающейся их должностных обязанностей.

5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ.

При передаче персональных данных сотрудники Общества должны соблюдать следующие требования:

Передача внешнему потребителю:

- передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
- передача персональных данных от держателя или его представителей внешнему потребителю может допускаться только с согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством РФ.

- ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения генерального директора и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;
- не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;
- по возможности персональные данные обезличиваются.

Передача внутреннему потребителю.

Общество вправе разрешать доступ к персональным данным внутреннему потребителю. Внутренние потребители персональных данных должны подписать обязательство о неразглашении персональных данных (Приложение №1).

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ.

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Общества.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

Для выбора и реализации методов и способов защиты информации в информационных системах Обществом назначено должностное лицо (сотрудник), ответственное за обеспечение безопасности персональных данных.

Выбор и реализация методов и способов защиты информации в информационных системах осуществляются на основе определяемых Обществом угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 г. № 55/86/20.

Классификация осуществляется по двум основным критериям: категории и объему обрабатываемых данных. В соответствии с требованиями ФСТЭК России выделены следующие категории персональных данных:

категория 1 - персональные данные, касающиеся расовой принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

категория 4 - обезличенные персональные данные.

С точки зрения объема обрабатываемых данных выделяются следующие виды систем:

категория 1 - в информационной системе одновременно обрабатываются персональные данные более 100 000 субъектов;

категория 2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100 000 субъектов;

категория 3 - в информационной системе одновременно обрабатываются персональные данные менее чем 1000 субъектов.

На основе установленного класса информационной системы определяются требования, которым она должна соответствовать.

6.1. «ВНУТРЕННЯЯ ЗАЩИТА».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Общества**.**

Для защиты персональных данных сотрудников и клиентов необходимо соблюдать ряд мер:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных;
- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний (персональных данных);
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований законодательства РФ о персональных данных, в том числе требований к защите персональных данных;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация режима обеспечения безопасности в помещениях, обеспечивающего сохранность носителей персональных данных и средств защиты информации и исключающего возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделений;
- воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

6.2. «ВНЕШНЯЯ ЗАЩИТА».

Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Общества, посетители.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

Для защиты персональных данных сотрудников и клиентов Общества необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим Общества;
- порядок охраны территории, зданий, помещений, транспортных средств.

7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ.

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый сотрудник Общества, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

Настоящая Политика, а также все изменения и дополнения к ней утверждаются приказом генерального директора Общества.

Настоящая Политика вступает в силу с даты утверждения генеральным директором.

Вопросы, которые не урегулированы настоящей Политикой, разрешаются в соответствии с законодательством Российской Федерации.

Настоящая Политика подлежит публикации в информационно-телекоммуникационной сети «Интернет» на официальном сайте Общества.