УТВЕРЖДЕНО
Приказом Генерального директора
ООО «Альянс Поволжье»
Васильевой Т.В.
от 01 июня 2019 г.

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ ЗАЩИТЫ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОСТАВЛЯЮЩИХ КОММЕРЧЕСКУЮ ТАЙНУ
ООО «Альянс Поволжье»

Город Чебоксары
2019 г.

1. Общие положения

1.1. Положение об организации защиты сведений конфиденциального характера, составляющих коммерческую тайну ООО «Альянс Поволжье» (далее – Положение) разработано в соответствии с Конституцией РФ, Гражданским кодексом РФ, Трудовым кодексом РФ, другими нормативно-правовыми актами Российской Федерации, регулирующими отношения в области информации, Уставом ООО «Альянс Поволжье» (далее – Общество).

1.2. Положение вводит категорирование информации, в зависимости от степени конфиденциальности и определяет режим конфиденциальности в Обществе по отношению к информации, содержащей сведения конфиденциального характера, хранимой и обрабатываемой в Обществе, и регламентирует меры по ее защите, с целью предотвращения нанесения возможного ущерба интересам и деловой репутации Общества, вызванного умышленными или неосторожными действиями работников Общества, других юридических и физических лиц вследствие разглашения (передачи, утраты) или незаконного присвоения такой информации.

1.3. Положение является руководящим документом, единым для всего Общества, обязательным для выполнения всеми работниками Общества. Положением определяются обязанности работников и должностных лиц Общества по обеспечению режима конфиденциальности, и вводится ответственность за нарушение этого режима.

1.4. Сохранение сведений конфиденциального характера является неотъемлемой частью

1.5. деятельности Общества.

1.6. Защита сведений конфиденциального характера не может быть использована для сокрытия фактов бесхозяйственности, недобросовестной конкуренции и других негативных явлений в деятельности Общества.

1.7. Настоящее Положение вступает в силу с момента его утверждения Приказом генерального директора Общества и действует без ограничения срока, до замены его новым Положением.

2. Термины и определения

2.1. Информация: сведения (сообщения, данные) независимо от формы их представления.

2.2. Документ (документированная информация): зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель.

2.3. Носитель информации: материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

2.4. Обладатель информации: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

2.5. Конфиденциальность информации: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2.6. Режим конфиденциальности: организационные, технические и иные меры по защите конфиденциальной информации, принимаемые ее обладателем на основании закона. Предметом рассмотрения данного Положения является документированная информация.

2.7. Доступ к информации: возможность получения информации и ее использования.

2.8. Информация, составляющая коммерческую тайну: сведения любого характера (технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в сфере деятельности Общества, а также сведения о

способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

2.9. Персональные данные: любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.10. Обезличивание персональных данных: действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2.11. Общедоступные персональные данные: персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.12. Политика безопасности (информации в организации): совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

3. Категорирование информации по степени конфиденциальности

Данным Положением в Обществе вводятся следующие категории информации:

- информация, содержащая сведения, составляющие охраняемую законом тайну (государственную, служебную, профессиональную, коммерческую или иную тайну);
- внутренняя информация ограниченного распространения (обращения);
- общедоступная информация.

3.1. Информация, содержащая сведения, составляющие охраняемую законом тайну (далее – ИОЗТ).

Информация, содержащая сведения, составляющие охраняемую законом тайну – это информация, содержащая сведения конфиденциального характера, доступ к которой должен быть ограничен и приняты меры по ее защите, в соответствии с требованиями Федеральных законов к ней относится:

- информация, составляющая коммерческую тайну Общества;
- информация, составляющая государственную тайну;
- персональные данные работников Общества.

3.1.1. Информация, составляющая коммерческую тайну Общества.

Право на отнесение информации к информации, составляющей коммерческую тайну и на определение перечня и состава такой информации, принадлежит Обществу, за исключением информации, содержащей сведения, перечисленные в статье 5 Федерального закона Российской Федерации от 29 июля 2004 г. №98-ФЗ «О коммерческой тайне».

Сведения, составляющие коммерческую тайну, определяются «Перечнем сведений, составляющих коммерческую тайну ООО «Альянс Поволжье» (далее – Перечень СКТ).

Перечень СКТ, является единым для всего Общества и утверждается приказом директора Общества.

Изменения и дополнения к Перечню вносятся в него приказом генерального директора Общества.

3.1.2. Персональные данные работников Общества.

Информация, содержащая персональные данные всегда относится к категории конфиденциальной информации, за исключением случаев:

- обезличивания персональных данных;
- иных случаях установленных Федеральным законом «О персональных данных» и иными федеральными нормативными актами.

Обработка персональных данных осуществляется в порядке и на условиях, предусмотренных действующим законодательством, при условии письменного согласия работника, содержащего перечень персональных данных и цель их обработки.

Исключение составляет случай, когда обработка персональных данных осуществляется в целях исполнения трудового или гражданско-правового договора с субъектом персональных данных.

Согласие, подписанное работником, приобщается к его личному делу и хранится в течение всего срока, определенного для хранения личных дел.

3.2. Внутренняя информация ограниченного распространения (обращения) (далее – ВИОР). К данной категории относится:

3.2.1. Внутренняя информация, которая не содержит сведений конфиденциального характера, распространение (обращение) которой в Обществе (вне Общества), может быть ограничено, исходя из интересов Общества или его структурных подразделений, если это не противоречит действующему законодательству РФ.

Перечень такой информации утверждается приказом директора Общества.

3.2.2. Информация, полученная от третьей стороны на основании договора и на условиях сохранения ее конфиденциальности.

Информация, полученная от третьей стороны, может быть отнесена к данной категории при одновременном соблюдении следующих условий:

- требования третьей стороны о соблюдении конфиденциальности передаваемой информации не противоречат действующему законодательству РФ;
- передача и получение информации осуществляется на основании договора;
- этим договором или отдельным соглашением к нему определены обязательства Общества по сохранению конфиденциальности и ответственность за разглашение этой информации.

Порядок изготовления, регистрации, учета, размножения, хранения и уничтожения документов, содержащих ВИОР, соответствует порядку для обычных документов и определяется Инструкцией по делопроизводству Общества.

Передача (обращение, распространение) документов, содержащих ВИОР внутри Общества (между структурными подразделениями) и третьим лицам должна осуществляться только с разрешения директора и только с сопроводительным письмом, содержащим предупреждение об ограничении распространения (обращения) документа, после обязательной регистрации в журнале исходящих документов.

Дополнительные меры по защите этой категории информации не предусматриваются.

3.3. Общедоступная информация.

К данной категории относится любая другая информация, не отнесенная к первым двум категориям, а также информация, определяемая Федеральным законодательством как общедоступная.

4. Организация работы по защите конфиденциальной информации

4.1. Организация работы по защите ИОЗТ (установлению режима конфиденциальности) Общества и контроль над соблюдением режима конфиденциальности и мер по ее защите, возложена на директора. В этой части директор выполняет следующие функции:

- разработка проектов руководящих документов по вопросам обеспечения режима конфиденциальности, определения порядка обращения с ИОЗТ;
- организация взаимодействия с органами государственной власти, правоохранительными и контролирующими органами, подразделениями безопасности и защиты информации

других организаций, координация работы структурных подразделений по вопросам обеспечения и соблюдения режима конфиденциальности;

- переработка (внесение изменений и дополнений) Перечня сведений, составляющих коммерческую тайну;
- рассмотрение возможности передачи ИОЗТ Общества, третьим лицам;
- рассмотрение предложений о снятии ограничений на доступ к информации, составляющей коммерческую тайну, а также о возможности опубликования такой информации на общедоступных ресурсах (раскрытия);
- установление требований к техническому оснащению помещений, в которых осуществляется работа с ИОЗТ;
- организация освидетельствования (приемки) помещений на предмет их пригодности к проведению работ с ИОЗТ;
- оценку (самостоятельно или с привлечением специалистов и организаций, в том числе на договорной основе) достаточности принимаемых в Обществе мер по обеспечению режима конфиденциальности;
- анализ и оценка рисков, связанных с нарушением режима конфиденциальности;
- проведение занятий и консультаций сотрудников Общества, по порядку и правилам обращения с ИОЗТ;
- рассмотрение вопросов обеспечения и соблюдения режима конфиденциальности.

4.2. Для выполнения указанных выше функций директор:

- привлекает отдельных специалистов для подготовки проектов локальных нормативных документов по защите ИОЗТ;
- производит плановые и внезапные проверки на предмет соблюдения режима конфиденциальности в Обществе;
- запрашивает от всех сотрудников Общества точного выполнения нормативных документов по обеспечению режима конфиденциальности. При необходимости - отстраняет от работы с ИОЗТ работников Общества, нарушающих установленные требования по соблюдению режима конфиденциальности, и запрещению обработки ИОЗТ техническими средствами, не обеспечивающими ее защиту от несанкционированного доступа.

5. Меры по защите ИОЗТ

Защита ИОЗТ Общества, обеспечивается комплексным использованием административных, организационных и технических мер защиты, в том числе:

- определением порядка отнесения сведений к сведениям, составляющим коммерческую тайну, определением и утверждением Перечня таких сведений;
- учетом лиц, получивших доступ к ИОЗТ, и (или) лиц, которым такая информация была предоставлена или передана;
- определением порядка регистрации, учета, размножения, хранения, передачи и уничтожения ИОЗТ и носителей такой информации;
- ограничением доступа к ИОЗТ;
- регулированием отношений по использованию ИОЗТ работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- определением обязанностей работников Общества при работе с ИОЗТ;
- установлением ответственности за разглашение ИОЗТ;
- назначением в структурных подразделениях Общества лиц, ответственных за обеспечение режима конфиденциальности, ведения конфиденциального делопроизводства и контроля над соблюдением режима конфиденциальности в этих подразделениях;

- нанесением на материальные носители (документы), содержащие ИОЗТ, грифа конфиденциальности.

5.1. Допуск работников Общества к работе с ИОЗТ.

5.1.1. Руководитель структурного подразделения формирует список работников своего подразделения, которых необходимо допустить к работе с ИОЗТ.

5.1.2. Окончательное решение о допуске к работе с ИОЗТ по каждому работнику принимается после подписания этим работником Обязательства о неразглашении конфиденциальной информации (далее – Обязательство) и ознакомления под роспись с Перечнем СКТ, настоящим Положением и Инструкциями. Обязательство, подписанное работником, приобщается к личному делу работника.

5.1.3. Список работников Общества, допущенных к работе с ИОЗТ, утверждается приказом директора Общества. Список подлежит обязательному пересмотру не реже одного раза в год. В течение этого периода в него могут вноситься изменения и дополнения по инициативе руководителей структурных подразделений Общества.

5.2. Требования к помещениям, в которых обрабатывается и хранится ИОЗТ.

5.2.1. Помещения должны располагаться в пределах охраняемого периметра зданий, и оборудованы средствами охранной и пожарной сигнализации;

5.2.2. Окна в помещениях должны быть оборудованы защитными жалюзи или пленками, защищающими от визуального контроля. Окна помещений, расположенных на первых и последних этажах зданий должны быть оборудованы защитными металлическими решетками;

5.2.3. Для хранения документов и носителей информации, содержащих ИОЗТ, в помещениях должны быть установлены сейфы или запираемые на замок металлические шкафы.

5.2.4. Помещения, в которых ведется прием посетителей, должны быть оборудованы защитными барьерами, ограничивающими рабочую зону и предотвращающими свободный проход в нее. При отсутствии таких барьеров работа с документами, содержащими ИОЗТ должна прекращаться на время приема посетителей.

5.2.5. Не допускается использование в этих помещениях фото-, теле-, видео-, радио аппаратуры, средств аудиозаписи, телефонов (факсов) с радио удлинителями, периферийных беспроводных компьютерных устройств во время работы с ИОЗТ.

5.3. Обработка и хранение конфиденциальной информации, представленной в электронном виде.

Конфиденциальная информация представленная в электронном виде может содержаться в отдельных электронных документах (файлах) или в составе баз данных.

5.3.1. Обработка и хранение ИОЗТ допускается только на отдельном, выделенном для этих целей сервере (серверах) информационно - вычислительной сети Общества (далее – ИВС) – сервере (серверах) конфиденциальной информации (далее – СКИ).

5.3.2. Обмен данными между СКИ и другими компьютерами (рабочими станциями, серверами) должен быть организован через защищенные соединения, организованные с использованием протоколов IPSec с проверкой подлинности и шифрованием IP-пакетов.

5.3.3. Запрещается копирование файлов с ИОЗТ и хранение их на жестких дисках рабочих станций (компьютеров, ноутбуков), съемных машинных носителях информации, других устройствах, способных накапливать и хранить информацию в электронном виде, за исключением случаев, описанных в Инструкциях.

5.3.4. Резервное копирование ИОЗТ с СКИ должно производиться на отдельные съемные носители информации.

5.3.5. Администрирование СКИ, внесение изменений в программное и аппаратное обеспечение, резервное копирование и восстановление информации должно осуществляться работниками Общества из числа допущенных к работе с конфиденциальной информацией.

5.3.6. Рабочие станции (компьютеры, ноутбуки) пользователей ИВС Общества, работающих с ИОЗТ допускается устанавливать в помещениях, отвечающих требованиям, описанным в подпункте 5.3. настоящего Положения.

5.3.7. Пользователям ИВС Общества (учетным записям пользователей), работающим с ИОЗТ должны быть запрещены доступ к сети Интернет, и средствам электронной почты.

5.4. Ограничение доступа к ИОЗТ.

5.4.1. Доступ к ИОЗТ должен предоставляться только тем лицам, которым эта информация необходима для выполнения возложенных на них обязанностей и только в том объеме (к той ее части), который необходим для выполнения определенных функций.

5.4.2. Правом предоставления, ограничения, прекращения доступа ко всей ИОЗТ, создаваемой, хранимой и обрабатываемой Обществом, включая информацию, полученную от третьих лиц, обладает директор Общества.

5.4.3. Правила и порядок предоставления и контроля доступа к информации определяются другими организационно - распорядительными документами Общества.

5.5. Порядок передачи конфиденциальной информации.

5.5.1. ИОЗТ может быть передана третьей стороне по письменному запросу третьей стороны и только с письменного разрешения директора Общества при условии соблюдения требований действующего законодательства:

- по требованию органов государственной власти и местного самоуправления, государственных надзорных и контролирующих органов, а также членов Общества в соответствии с действующим законодательством РФ;
- членам других органов Общества в соответствии с уставом Общества;
- другим физическим и юридическим лицам на основании гражданско-правовых договоров, заключенных между ними и Обществом, при условии наличия в этих договорах обязательств по соблюдению режима конфиденциальности в отношении данной информации, ответственности за разглашение этой информации или заключения с ними отдельного договора о конфиденциальности.

5.5.2. Необходимость (возможность) передачи ИОЗТ Общества для открытого опубликования (раскрытия), ее объем, форму, и время опубликования (раскрытия) определяет директор Общества. Под открытым опубликованием (раскрытием) ИОЗТ понимается ее публикация в открытой печати, компьютерных информационных сетях общего пользования, передача по радио и телевидению, оглашение на международных и российских симпозиумах, совещаниях, конференциях, съездах, при публичных выступлениях, вывоз за границу или передача ее в любой форме организациям или отдельным лицам, с которыми не заключен договор о конфиденциальности.

5.5.3. Персональные данные работников Общества могут быть переданы третьей стороне или опубликованы на общедоступных источниках только с письменного согласия этих работников на передачу или опубликование своих персональных данных. В случае передачи персональных данных третьим лицам, эти лица должны быть предупреждены о необходимости соблюдать конфиденциальность полученных персональных данных.

5.5.4. Порядок передачи ИОЗТ внутри Общества и третьим лицам на бумажных и съемных машинных носителях информации определяется Инструкциями. Передача ИОЗТ, представленной в электронном виде (документы, файлы, базы данных, архивы) через сети передачи данных должна осуществляться исключительно в зашифрованном виде, при условии, что только обменивающимся сторонам доступны секретные ключи шифрования (пароли).

5.6. Порядок подготовки и проведения совещаний, встреч, переговоров, аудио и видеоконференций, связанных с обсуждением сведений конфиденциального характера.

Проведение совещаний, встреч, переговоров, аудио и видеоконференций, телефонных переговоров связанных с обсуждением сведений конфиденциального характера без принятия специальных мер, изложенных ниже, не допускается:

- совещания, встречи, переговоры, аудио и видеоконференции, связанные с обсуждением сведений конфиденциального характера должны проводиться в специально выделенных для этих целей помещениях (далее – ВП). Перечень таких помещений утверждается директором Общества;
- доступ в ВП должен быть ограничен кругом лиц, участвующих (приглашенных) в совещании;
- запрещается проведение аудио- и видеоконференций, связанных с обсуждением сведений конфиденциального характера без принятия специальных мер защиты информации, передаваемой по незащищенным каналам связи;
- запрещается использование фото-, видео-, аудиозаписи, мобильных телефонов, диктофонов и других технических средств регистрации информации, в том числе, встроенных в портативные и карманные компьютеры, мобильные телефоны, без разрешения должностного лица Общества, ответственного за проведение мероприятия;
- должностные лица Общества, ответственные за проведение мероприятий обязаны ознакомить всех участников с требованиями настоящего Положения об ограничениях в использовании технических средств регистрации информации, о необходимости сохранения в тайне сведений конфиденциального характера (при необходимости уточнить какие именно сведения являются охраняемыми), о чем делается отметка в протоколе совещания (встречи, переговоров, аудио и видеоконференции).

5.7. Обязанности работников Общества, допущенных к работе с ИОЗТ.

5.7.1. Работник Общества, допущенный к работе с ИОЗТ, обязан:

- знать и выполнять требования настоящего Положения, других руководящих документов по защите информации, а также знать Перечень сведений, составляющих коммерческую тайну Общества;
- соблюдать порядок работы и меры по защите ставших ему известными сведений конфиденциального характера;
- немедленно, в письменной форме, информировать директора, руководителя соответствующего структурного подразделения:
  - о попытках несанкционированного доступа к информационным ресурсам и сведениям, составляющим коммерческую тайну Общества, и персональным данным;
  - о попытках подкупа, угроз, шантажа другими лицами с целью получения доступа к конфиденциальной информации;
- немедленно представлять директору письменные объяснения о допущенных личных нарушениях установленного порядка работы, учета и хранения документов с ИОЗТ и машинных съемных носителей информации, а также о фактах их утраты, передачи другим лицам, в том числе случайной;
- строго соблюдать правила работы с носителями ИОЗТ Общества, порядок их учета и хранения, обеспечивать в процессе работы сохранность сведений, содержащихся в них от посторонних лиц;
- знакомиться только с теми сведениями, к которым получен доступ в связи с исполнением своих трудовых обязанностей.

5.7.2. Работнику, допущенному к работе с ИОЗТ, запрещается:

- передавать без разрешения руководителя структурного подразделения сведения конфиденциального характера и документы (в устной форме, по телефону, на бумажных и машинных носителях, в электронной виде и т.д.) другим лицам;
- использовать ИОЗТ Общества в открытой переписке, статьях и выступлениях, а также в личных интересах;
- передавать по незащищенным техническим каналам связи, в том числе сообщать (обсуждать) по телефону сведения конфиденциального характера;
- снимать копии с документов, содержащих ИОЗТ или производить выписки из них без разрешения руководителя структурного подразделения;

- копировать ИОЗТ Общества и хранить ее на машинных съемных носителях информации, а также использовать различные технические средства, способные накапливать и хранить информацию в электронном виде (фото, видео и звукозаписывающую аппаратуру, сотовые телефоны и т.п.), за исключением случаев, описанных в Инструкциях;
- выполнять работы с ИОЗТ вне служебных помещений (помещений, где размещены подразделения Общества) без разрешения руководителя структурного подразделения;
- выносить из служебных помещений документы и машинные носители с ИОЗТ без разрешения руководителя структурного подразделения.

6. Обязанности руководителей структурных подразделений Общества по обеспечению режима конфиденциальности

Руководители структурных подразделений отвечают за обеспечение режима конфиденциальности, они обязаны:

- вносить предложения на внесение (исключение) в Перечень сведений, составляющих коммерческую тайну Общества;
- организовать в подчиненных подразделениях работу по обеспечению сохранения в тайне ИОЗТ, анализировать состояние этой работы, принимать меры по предупреждению нарушений режима конфиденциальности;
- определять права и полномочия (копирование, редактирование, уничтожение и т.п) работников своего и других подразделений по доступу к ИОЗТ Общества, в том числе в имеющихся и создаваемых базах данных, вести учет предоставленного доступа, вносить соответствующие изменения и дополнения в должностные инструкции подчиненных работников;
- контролировать состояние режима конфиденциальности в своем подразделении;
- организовывать обучение сотрудников своего подразделения порядку и правилам обращения с ИОЗТ Общества;
- организовать и контролировать учет, хранение, уничтожение документов и машинных носителей с ИОЗТ;
- не реже одного раза в квартал проверять наличие документов и зарегистрированных машинных носителей с ИОЗТ.

7. Ответственность за нарушение режима конфиденциальности

7.1. Работники Общества несут персональную ответственность за нарушение режима конфиденциальности, установленного в Обществе.

7.2. Нарушение режима конфиденциальности, приведшее или способное привести к разглашению конфиденциальной информации, является чрезвычайным происшествиями влечет за собой последствия, предусмотренные подписанным работником Обязательством и действующим законодательством РФ.

7.3. По всем фактам нарушений режима конфиденциальности должны быть проведены расследования, в ходе которых определен круг лиц, виновных в этих нарушениях и причастных к ним, а также причины и условия, способствовавшие совершению данных нарушений, и приняты соответствующие меры. Для этого:

- приказом директора создается комиссия, которая в срок не более 5 календарных дней со дня обнаружения факта нарушения проводит расследование и представляет материалы этого расследования директору Общества;
- одновременно с работой комиссии руководителями структурных подразделений должны быть приняты меры по локализации отрицательных последствий от данного нарушения;

- на основании результатов проведенного расследования директор Общества принимает решение о применении к виновным лицам мер материальной и/или иной ответственности в порядке, предусмотренном действующим законодательством РФ.

7.4. Виновные в нарушении режима конфиденциальности, повлекшем (способном повлечь) за собой разглашение ИОЗТ, в соответствии с законодательством РФ могут быть привлечены к дисциплинарной, административной или уголовной ответственности.

Прошито и пронумеровано
и скреплено печатью на стр.
Генеральный директор
Васильева Т.В. _____ (Подпись)
М.П.
«01» июня 2019 года