CONTACT CENTRE
CONNECT LINE

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

Приложение к приказу от 24.02.2023г №05
УТВЕРЖДАЮ
Генеральный директор
ООО "Коннект Лайн"
_____ Галинкин А.А.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «КОННЕКТ ЛАЙН»»

Определения.

В настоящем документе используются следующие термины и их определения:

- **Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
- **Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.
- **Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.
- **Биометрические персональные данные** – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.
- **Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.
- **Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.
- **Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.
- **Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

- **Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.
- **Доступ к информации** – возможность получения информации и ее использования.
- **Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).
- **Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
- **Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
- **Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.
- **Информационная система** персональных данных (ИСПДн) – 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.
- **Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
- **Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.
- **Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.
- **Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.
- **Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

- **Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.
- **Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.
- **Неавтоматизированная обработка персональных данных** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
- **Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.
- **Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.
- **Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
- **Обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.
- **Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
- **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.
- **Оператор (персональных данных)** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.
- **Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

- **Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.
- **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.
- **Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.
- **Политика «чистого стола»** – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.
- **Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.
- **Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
- **Программная закладка** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.
- **Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.
- **Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.
- **Распространение персональных данных** – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.
- **Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

- **Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.
- **Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
- **Субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- **Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.
- **Трансграничная передача персональных данных** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.
- **Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.
- **Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.
- **Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.
- **Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.
- **Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Обозначения и сокращения.

- АВС – антивирусные средства
- АРМ —автоматизированное рабочее место
- ВТСС – вспомогательные технические средства и системы
- ИСПДн – информационная система персональных данных
- КЗ – контролируемая зона
- ЛВС – локальная вычислительная сеть

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

- МЭ – межсетевой экран
- НСД – несанкционированный доступ
- ОС – операционная система
- ПДн – персональные данные
- ПМВ – программно-математическое воздействие
- ПО – программное обеспечение
- ПЭМИН – побочные электромагнитные излучения и наводки
- САЗ – система анализа защищенности
- СЗИ – средства защиты информации
- СЗПДн – система (подсистема) защиты персональных данных
- СОВ – система обнаружения вторжений
- ТКУ И – технические каналы утечки информации
- УБПДн – угрозы безопасности персональных данных

Введение.

Настоящая Политика информационной безопасности (далее – Политика) Общества с ограниченной ответственностью «Коннект Лайн» (далее - Организация) является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Концепции информационной безопасности ИСПД Организации.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 11 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», на основании:

- «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных Заместителем директора ФСТЭК России от 15.02.2008 г.,
- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Организации.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

1. **Общие положения.**
   1.1. Целью настоящей Политики является обеспечение безопасности объектов защиты Организации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).
   1.2. 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.
   1.3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.
   1.4. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.
   1.5. Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

2. **Область действия.**
   2.1. Требования настоящей Политики распространяются на всех сотрудников Организации (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. **Система защиты персональных данных.**
   3.1. Система защиты персональных данных (СЗПДн), строится на основании:
      3.1.1. Отчета о результатах проведения внутренней проверки;
      3.1.2. Перечня персональных данных, подлежащих защите;
      3.1.3. Акта классификации информационной системы персональных данных;
      3.1.4. Модели угроз безопасности персональных данных;
      3.1.5. Положения о разграничении прав доступа к обрабатываемым персональным данным;
      3.1.6. Руководящих документов ФСТЭК и ФСБ России.
   3.2. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Организации. На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз и Отчета о результатах проведения внутренней проверке, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.
   3.3. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:
      3.3.1. АРМ пользователей;

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

3.3.2. Сервера приложений;
3.3.3. СУБД;
3.3.4. Граница ЛВС;
3.3.5. Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

3.4. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:
- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

3.5. Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:
- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;

3.6. Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем Организации или лицом, ответственным за обеспечение защиты ПДн.

4. Требования к подсистемам СЗПДн.

СЗПДн включает в себя следующие подсистемы:
- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных.

4.1. Подсистемы управления доступом, регистрации и учета.

4.1.1. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:
- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее остановка.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

4.1.2. Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

4.2. Подсистема обеспечения целостности и доступности.

4.2.1. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Организации, а также средств защиты, при случайной или намеренной модификации.

4.2.2. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

4.3. Подсистема антивирусной защиты.

4.3.1. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Организации.

4.3.2. Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

4.3.3. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

4.4. Подсистема межсетевого экранирования.

4.4.1. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по следующим параметрам;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
- идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;
- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- контроля целостности своей программной и информационной части;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

4.4.2. Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛСВ, классом не ниже 4.

4.5. Подсистема анализа защищенности.

4.5.1. Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

4.5.2. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

4.6. Подсистема обнаружения вторжений.

4.6.1. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

4.6.2. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

4.7. Подсистема криптографической защиты.

4.7.1. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Организации, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

4.7.2. Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

5. Пользователи ИСПДн.

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн Организации можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;
- Администратора безопасности;
- Оператора АРМ;
- Администратора сети;
- Технического специалиста по обслуживанию периферийного оборудования;
- Программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным.

5.1. Администратор ИСПДн.

5.1.1. Администратор ИСПДн, сотрудник Организации, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

5.1.2. Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

5.2. Администратор безопасности.

5.2.1. Администратор безопасности, сотрудник Организации, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

5.2.2. Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

5.2.3. Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других организаций.

5.3. Оператор АРМ.

5.3.1. Оператор АРМ, сотрудник Организации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

5.3.2. Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

5.4. Администратор сети.

5.4.1. Администратор сети, сотрудник Организации, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

5.4.2. Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

- знает, по меньшей мере, одно легальное имя доступа.

5.5. Технический специалист по обслуживанию периферийного оборудования.

5.5.1. Технический специалист по обслуживанию, сотрудник Организации, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

5.5.2. Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

5.6. Программист-разработчик ИСПДн.

5.6.1. Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Организации, так и сотрудники сторонних организаций.

5.6.2. Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

6. Требования к персоналу по обеспечению защиты ПДн.

6.1. Все сотрудники Организации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

6.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

6.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

6.4. Сотрудники Организации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

6.5. Сотрудники Организации должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

6.6. Сотрудники Организации должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

6.7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

6.8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Организации, третьим лицам.

6.9. При работе с ПДн в ИСПДн сотрудники Организации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

6.10. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

6.11. Сотрудники Организации должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

6.12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн

7. Должностные обязанности пользователей ИСПДн.

7.1. Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

8. Ответственность сотрудников ИСПДн Организации.

8.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

8.2. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

8.3. Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

8.4. При нарушениях сотрудниками Организации – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

8.5. Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях Организации, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Организации.

Приложение 1

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К3	К2	К1
I	В подсистеме управления доступом:			
1	Реализовать идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;	+	+	+
2	Реализовать идентификацию терминалов, технических средств обработки ПДн, узлов ИСПДн, компьютеров, каналов связи, внешних устройств ИСПДн по их логическим именам (адресам, номерам);	-	+	+
3	Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам;	-	+	+
4	Реализовать контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;	-	+	+
5	при наличии подключения ИСПДн к сетям общего пользования должно применяться межсетевое экранирование.	Не ниже 5-го уровня защищенности	Не ниже 4-го уровня защищенности	Не ниже 3-го уровня защищенности
6	Для обеспечения безопасного межсетевого взаимодействия в ИСПДн для разных классов необходимо использовать МЭ	Не ниже 5-го уровня защищенности	Не ниже 4-го уровня защищенности	Не ниже 3-го уровня защищенности
II	Средство защиты от программно-математических воздействий (ПМВ):			
1	Реализовать идентификацию и аутентификацию субъектов доступа при входе в средство защиты от программно-математических воздействий (ПМВ) и перед выполнением ими любых операций по управлению функциями средства защиты от ПМВ по паролю (или с использованием иного механизма аутентификации) условно-постоянного действия длиной не менее шести буквенно-цифровых символов;	+	+	+

2	Осуществлять контроль любых действий субъектов доступа по управлению функциями средства защиты от ПМВ только после проведения его успешной аутентификации;	+	+	+
3	Предусмотреть механизмы блокирования доступа к средствам защиты от ПМВ при выполнении устанавливаемого числа неудачных попыток ввода пароля;	+	+	+
4	Необходимо проводить идентификацию файлов, каталогов, программных модулей, внешних устройств, используемых средств защиты от ПМВ;	+	+	+
III	В подсистеме регистрации и учета:			
1	Осуществлять регистрацию входа (выхода) субъекта доступа в систему (из системы), либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;	+	+	+
2	Проводить учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку);	+	+	+
3	Проводить регистрацию входа/выхода субъектов доступа в средство защиты от ПМВ, регистрацию загрузки и инициализации этого средства и ее программного останова. В параметрах регистрации указывается время и дата входа/выхода субъекта доступа в средство защиты от ПМВ или загрузки/останова этого средства, а также идентификатор субъекта доступа, инициировавшего данные действия;	+	+	+
4	Проводить регистрацию событий проверки и обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы (ВП), результат действий средства защиты по блокированию ПМВ;	+	+	+

5	Проводить регистрацию событий по внедрению в средство защиты от ПМВ пакетов обновлений. В параметрах регистрации указываются время и дата обновления, идентификатор субъекта доступа, инициировавшего данное действие версия и контрольная сумма пакета обновления;	+	+	+
6	Проводить регистрацию событий запуска/завершения работы модулей средства защиты от ПМВ. В параметрах регистрации указываются время и дата запуска/завершения работы, идентификатор модуля, идентификатор субъекта доступа, инициировавшего данное действие, результат запуска/завершения работы;	+	+	+
7	должна проводиться регистрация событий управления субъектом доступа функциями средства защиты от ПМВ. В параметрах регистрации указываются время и дата события управления каждой функцией, идентификатор и спецификация функции, идентификатор субъекта доступа, инициировавшего данное действие, результат действия;	+	+	+
8	Проводить регистрацию событий попыток доступа программных средств к модулям средства защиты от ПМВ или специальным ловушкам. В параметрах регистрации указываются время и дата попытки доступа, идентификатор модуля, идентификатор и спецификация модуля средства защиты от ПМВ (специальной ловушки), результат попытки доступа;	+	+	+
9	Проводить регистрацию событий отката для средства защиты от ПМВ. В параметрах регистрации указываются время и дата события отката, спецификация действий отката, идентификатор субъекта доступа, инициировавшего данное действие, результат действия;	+	+	+
10	Обеспечить защиту данных регистрации от их уничтожения или модификации нарушителем;	+	+	+
11	Реализовать механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов;	+	+	+

12	Реализовать механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров;	+	+	+
13	Проводить автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВП).	+	+	+
14	Реализовать механизм автоматического анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением администратора безопасности;	+	+	+
15	Проводить несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;	+	+	+
16	Осуществлять регистрацию входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы.	-	+	+
17	Осуществлять регистрацию выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются (дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи – логическое имя (номер) внешнего устройства, краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ;	-	+	+
18	Осуществлять регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный – несанкционированный),	-	+	+

19	Осуществлять регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла;	-	+	+
20	Осуществлять регистрацию попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта – логическое имя (номер);	-	+	+
21	Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);	-	+	+
22	Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов, информации);	-	+	+
IV	В подсистеме обеспечения целостности:			
1	Обеспечить целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ;	+	+	+
2	Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;	+	+	+

3	Проводить периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;	+	+	+
4	должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;	+	+	+
5	Проводить проверку целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм;	+	+	+
6	Обеспечить возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности;	+	+	+
7	Реализовать механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;	+	+	+
8	Проводить резервное копирование ПДн на отчуждаемые носители информации;	-	+	+
V	В подсистеме антивирусной защиты:			
1	Проводить автоматическую проверку на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа;	+	+	+
2	Реализовать механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения;	+	+	+
3	Регулярно выполнять (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВП;	+	+	+

4	Должна инициироваться автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ;	+	+	+
5	Реализовать механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.	+	+	+
6	Дополнительно в ИСПДн должен проводиться непрерывный автоматический мониторинг информационного обмена с внешней сетью с целью выявления ВП.	+	+	+
VI	Контроль отсутствия НДВ в ПО СЗИ			
1	Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации – СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение – ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ (не декларированных возможностей).	+	+	+
VII	Обнаружение вторжений в ИСПДн			
	Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).	+	+	+
1	Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа	+	-	-
2	Необходимо обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа и методы выявления аномалий	-	+	+
VIII	Защита ИСПДн от ПЭМИН			
1	Для обработки информации необходимо использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216 91, ГОСТ Р 50948-2001, ГОСТ Р 50949-2001, ГОСТ Р 50923 96, СанПиН 2.2.2.542 96).	+	+	+
IX	Оценка соответствия ИСПДн требованиям безопасности ПДн			

1	Провести обязательную сертификацию (аттестацию) по требованиям безопасности информации;	-	+	+
2	Декларировать соответствие или обязательную сертификацию (аттестацию) по требованиям безопасности информации (по решению оператора);	+	-	-

Примечание: Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется в зависимости от ущерба, который может быть нанесен в следствии несанкционированного или непреднамеренного доступа к ПДн.

CONTACT CENTRE
CONNECT LINE

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

Приложение к приказу от 24.02.2023 г. за №05

УТВЕРЖДАЮ
Генеральный директор
ООО "Коннект Лайн"
_____ Галинкин А.А.

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПОДЛЕЖАЩИХ ЗАЩИТЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «КОННЕКТ ЛАЙН»»

Введение.

Настоящий Перечень персональных данных, подлежащих защите в информационных системах персональных данных (ИСПДн) (далее – Перечень) Общества с ограниченной ответственностью «Коннект Лайн» (далее – Организация) является официальным документом.

Перечень разработан в соответствии со списком объектов защиты, изложенных в Концепции информационной безопасности ИСПДн Организации.

Перечень содержит полный список категорий данных, безопасность которых должна обеспечиваться системой защиты персональных данных (СЗПДн).

1. Общие положения.

1.1. Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень объектов защиты определен по результатам Отчета о результатах проведения внутренней проверки.

1.2. Объекты защиты каждой ИСПДн включают:

1.2.1. Обрабатываемая информация:
- персональные данные субъектов ПДн (раздел 2.1.1);
- персональные данные сотрудников (раздел 2.1.2);

1.2.2. Технологическая информация (раздел 2.2).

1.2.3. Программно-технические средства обработки (раздел 2.3).

1.2.4. Средства защиты ПДн (раздел 2.4).

1.2.5. Каналы информационного обмена и телекоммуникации (раздел 2.5).

1.2.6. Объекты и помещения, в которых размещены компоненты ИСПДн (раздел 2.6).

2. ИСПДн.

2.1. Обрабатываемая информация.

2.1.1. Перечень персональных данных субъектов ПДн.

Персональные данные субъектов ПДн (клиентов) включают:
- ФИО;
- Дата рождения;

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

- Контактный телефон;
- Адрес прописки;
- Адрес фактического проживания;
- Паспортные данные;
- Данные о состоянии здоровья (история болезни).

2.1.2. Перечень персональных данных сотрудников Организации.

Персональные данные сотрудников Организации включают:

- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке;
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- Адрес проживания (реальный);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;
- Оклад;
- Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о приеме на работу, перемещении по должности, увольнении;
- Информация об отпусках;
- Информация о командировках;
- Информация о болезнях;
- Информация о негосударственном пенсионном обеспечении.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

2.2. Технологическая информация.

Технологическая информация, подлежащая защите, включает:

- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

2.3. Программно-технические средства обработки.

Программно-технические средства включают в себя:

- общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

2.4. Средства защиты ПДн.

Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передаче по каналам связи сетей общего и (или) международного обмена.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

2.5. Каналы информационного обмена и телекоммуникации.

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

2.6. Объекты и помещения, в которых размещены компоненты ИСПДн.

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

CONTACT CENTRE
CONNECT LINE

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

Приложение к приказу от 24.02.2023г №05
УТВЕРЖДАЮ
Генеральный директор
ООО "Коннект Лайн"
Галинкин А.А.

ПОЛОЖЕНИЕ «О ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЩЕСТВЕ С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «КОННЕКТ ЛАЙН»

1. Общие положения

1.1. Настоящее Положение определяет состав персональных данных, порядок получения, учета, обработки, накопления и хранения документов и других носителей, содержащих сведения, отнесенные к персональным данным передаваемых в Общество с ограниченной ответственностью «Коннект Лайн» (далее — «Компания») для выполнения последним договорных отношений, гарантии конфиденциальности сведений, предоставленных третьей стороной Компании.

1.2. Цель разработки настоящего Положения — определение порядка обработки полученных персональных данных, их защита от несанкционированного доступа, неправомерного использования, разглашения или утраты.

1.3. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускаются. Персональные данные требуют безопасной обработки.

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

1.5. Должностные лица, в обязанность которых входит ведение персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

1.6. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

1.7. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

1.8. Неправомерность деятельности органов государственной власти и организаций по сбору персональных данных может быть установлена в судебном порядке по требованию субъектов, действующих на основании статей 14 и 15 Федерального закона и законодательства о персональных данных.

1.9. Настоящее положение является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

2. Понятие и состав персональных данных.

2.1. Персональные данные — информация о физических лицах (далее – субъекты персональных данных), необходимая Компании в связи с исполнением трудовых и прочих договорных отношений и касающаяся конкретного гражданина.

2.2. Состав Персональных данных:

— анкетные и биографические данные;

— образование;

— сведения о трудовом и общем стаже;

— сведения о доходах и вознаграждениях;

— сведения о составе семьи;

— паспортные данные;

— сведения о воинском учете;

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

— сведения о заработной плате сотрудника;

— сведения о социальных льготах;

— специальность;

— занимаемая должность;

— наличие судимостей;

— адрес места жительства;

— домашний или мобильный телефон;

— место работы или учебы членов семьи и родственников;

— характер взаимоотношений в семье;

— 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 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.

3. Обязанности Компании

В целях обеспечения прав и свобод человека и гражданина организация и её представители при обработке персональных данных обязаны соблюдать следующие общие требования:

— обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов;

— при определении объема и содержания обрабатываемых персональных данных организация должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;

— все персональные данные следует получать у субъекта персональных данных. Если персональные данные возможно получить только у третьей

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Необходимо сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение;

— организация не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, организация вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

— при принятии решений, затрагивающих интересы субъекта, организация не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения;

— защита персональных данных субъекта от неправомерного их использования или утраты должна быть обеспечена организацией за счет его средств в порядке, установленном федеральным законом;

— работники и их представители должны быть ознакомлены под расписку с документами Компании, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

— субъекты не должны отказываться от своих прав на сохранение и защиту тайны.

4. Обязанности работников Компании

Работники Компании обязаны:

— передавать Компании или её представителю комплекс достоверных документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

— своевременно сообщать Компании об изменении своих персональных данных.

— соблюдать все требования Компании по защите персональных данных.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

5. Права субъекта персональных данных.

Субъект персональных данных имеем право:

— требовать исключения или исправления неверных или неполных персональных данных;

— на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;

— персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

— определять своих представителей для защиты своих персональных данных;

— на сохранение и защиту своей личной и семейной тайны.

6. Сбор, обработка и хранение персональных данных

6.1. Обработка персональных данных субъекта — получение, хранение, комбинирование, передача или любое другое использование персональных данных субъекта.

6.2. Порядок получения персональных данных.

6.2.1. Все персональные данные субъекта следует получать у него самого. Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть письменное согласие. Организация должна сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

6.2.2. Компания не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции РФ, Компания вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

6.2.3. Обработка, передача и хранение персональных данных субъекта.

К обработке, передаче и хранению персональных данных субъекта могут иметь

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

доступ сотрудники:

а) Генеральный Директор Компании;

б) сотрудники отдела кадров Компании;

в) сотрудники бухгалтерии;

г) сотрудники юридического отдела Компании;

д) сотрудники ИТ-служб Компании при выполнении своих должностных обязанностей.

6.2.4. При передаче персональных данных субъекта организация должны соблюдать следующие требования:

— не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральными законами;

— не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

— предупредить лиц, получающих персональные данные субъекта 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. Лица, получающие персональные данные субъекта, обязаны соблюдать режим безопасности. Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами;

— разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций;

— не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения субъектом трудовой функции;

— передавать персональные данные субъекта представителям субъектов в порядке, установленном законом, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

6.2.5. Передача персональных данных от субъекта или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

6.2.6. При передаче персональных данных субъекта потребителям (в том числе и в коммерческих целях) за пределы Компании, Компания не должна сообщать эти данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта или в случаях, установленных федеральными Законами.

6.2.7. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъекта распространяется как на бумажные, так и электронные (автоматизированные) носители информации.

6.2.8. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

6.2.9. По возможности персональные данные обезличиваются.

7. Доступ к персональным данным.

7.1. Внутренний доступ (доступ внутри Компании)

Право доступа к персональным данным имеют:

а) Генеральный Директор Компании;

б) сотрудники отдела кадров Компании;

в) сотрудники бухгалтерии;

г) сотрудники юридического отдела Компании;

д) сотрудники ИТ-служб Компании при выполнении своих должностных обязанностей.

7.2. Внешний доступ.

7.2.1. К числу массовых потребителей персональных данных вне Компании можно отнести государственные и негосударственные функциональные структуры:

— налоговые инспекции;

— правоохранительные органы;

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

— органы статистики;

— страховые агентства;

— военкоматы;

— органы социального страхования;

— пенсионные фонды;

— подразделения муниципальных органов управления;

7.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

7.2.3. Субъект, его родственники и члены семей.

Персональные данные субъекта могут быть предоставлены самому субъекту или с его письменного разрешения его родственникам или членам его семьи.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия, (УК РФ).

7.2.4. 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 жестко регламентированный и динамически 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 компании.

7.2.4.1. «Внутренняя зашита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

данных Регламентация доступа персонала к документам и базам данных с персональными сведениями входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами компании. Для защиты персональных данных субъектов необходимо соблюдать ряд мер:

— ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

— строгое избирательное и обоснованное распределение документов и информации между работниками;

— рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

— знание работником требований нормативно — методических документов по защите информации и сохранении тайны;

— наличие необходимых условий в помещении для работы с документами и базами данных с персональными сведениями;

— определение и регламентация 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 подразделения;

— воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждение утраты ценных сведений при работе с документами, содержащими персональные данные;

— все файлы, папки, базы данных и т.п. содержащие персональные данные, должны быть защищены паролем, который сообщается сотрудникам наделенным соответствующим приказом правом на обработку персональных данных.

7.2.4.2. «Внешняя защита».

Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

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 компании, посетители, работники других организационных структур,

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел, рабочих материалов и баз данных в отделах обрабатывающих персональные данные.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

— порядок приема, учета и контроля деятельности посетителей;

— пропускной режим компании;

— учет и порядок выдачи удостоверений;

— технические средства охраны, сигнализации;

— порядок охраны территории, зданий, помещений, транспортных средств;

— требования к защите информации при интервьюировании и собеседованиях.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

Все лица, связанные с получением, обработкой и защитой персональных данных обязаны заключить «Соглашение о неразглашении персональных данных».

8. Ответственость за разглашение персональных данных, информации связанной с персональными данными.

8.1. Персональная ответственность — одно из главных требований к Компании функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

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

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

8.4. Лица, виновные в нарушении установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) несут дисциплинарную, административную, гражданско—правовую или уголовную ответственность в соответствии с федеральными законами

CONTACT CENTRE
CONNECT LINE

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

Приложение 1.

Соглашение о неразглашении Персональных данных

Я, _____,
паспорт серия _____, номер _____,
выданный _____
«_____»_____ _____года, понимаю, что получаю доступ к персональным данным физических лиц, обрабатываемым в ООО «Коннект Лайн». Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъекту персональных данных как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сбором, обработкой и хранением) с персональными данными субъекта персональных данных соблюдать все описанные в «Положении о персональных данных в обществе с ограниченной ответственностью «Коннект Лайн»»

Я подтверждаю, что не имею права разглашать сведения:

1) анкетные и биографические данные;

2) образование;

3) сведения о трудовом и общем стаже;

4) сведения о доходах и вознаграждениях;

5) сведения о составе семьи;

6) паспортные данные;

7) сведения о воинском учете;

8) сведения о заработной плате;

9) сведения о социальных льготах;

10) специальность,

11) занимаемая должность;

12) наличие судимостей;

CONTACT CENTRE
CONNECT LINE

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

13) адрес места жительства;

14) домашний или мобильный телефон;

15) место работы или учебы членов семьи и родственников;

16) характер взаимоотношений в семье;

17) содержание трудового договора;

18) состав декларируемых сведений о наличии материальных ценностей;

19) содержание декларации, подаваемой в налоговую инспекцию;

20) подлинники и копии приказов по личному составу;

21) личные дела и трудовые книжки сотрудников;

22) основания к приказам по личному составу;

23) дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

24) копии отчетов, направляемые в органы статистики.

Я предупрежден(-а) о том, что в случае разглашения мной сведений, касающихся персональных данных субъекта персональных данных или их утраты, я несу ответственность в соответствии с федеральным законодательством.

С «Положении о персональных данных в обществе с ограниченной ответственностью «Коннект Лайн»» ознакомлен(а).

_____	_____	_____	«__»_____20__г.
(должность)	(ФИО)	(подпись)	(дата)

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

Приложение к приказу от 24.02.2023г. за №05
УТВЕРЖДАЮ
Генеральный директор
ООО "Коннект Лайн"
_____ Галинкин А.А.

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОСЕТИТЕЛЕЙ САЙТА

Посетитель сайта (далее – Пользователь), оставляя заявку на интернет-сайтах http://www.connect-line.ru, https://frontline-cc.ru/ принимает настоящее Согласие на обработку персональных данных (далее – Согласие). Действуя свободно, своей волей и в своем интересе, а также подтверждая свою дееспособность, Пользователь дает свое согласие Обществу с ограниченной ответственностью "Коннект Лайн" (ИНН 7704450680), которое расположено по адресу 115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский, ул.Ленинская слобода, д.19, оф.2031, ком.09 (далее – Общество), на обработку своих персональных данных со следующими условиями: Данное Согласие дается на обработку персональных данных, как без использования средств автоматизации, так и с их использованием.

1. Согласие дается на обработку следующих моих персональных данных: Персональные данные, не являющиеся специальными или биометрическими: номера контактных телефонов; адреса электронной почты; место работы и занимаемая должность; пользовательские данные (сведения о местоположении; тип и версия ОС; тип и версия Браузера; тип устройства и разрешение его экрана; источник откуда пришел на сайт пользователь; с какого сайта или по какой рекламе; язык ОС и Браузера; какие страницы открывает и на какие кнопки нажимает пользователь; ip-адрес.

2. Персональные данные не являются общедоступными.

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

3. Цель обработки персональных данных: обработка входящих запросов от физических лиц с целью трудоустройства в Общество и консультирования; обработка входящих запросов на предоставление услуг компании и приобретения программного обеспечения, аналитики действий физического лица на веб-сайте и функционирования веб-сайта; проведение рекламных и новостных рассылок.

4. Основанием для обработки персональных данных является: ст. 24 Конституции Российской Федерации; ст.6 Федерального закона №152-ФЗ «О персональных данных»; Устав Общества; настоящее согласие на обработку персональных данных

5. В ходе обработки с персональными данными будут совершены следующие действия: сбор; запись; систематизация; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; блокирование; удаление; уничтожение.

6. Персональные данные обрабатываются в течении 3 лет. Также обработка персональных данных может быть прекращена по запросу субъекта персональных данных. Хранение персональных данных, зафиксированных на бумажных носителях осуществляется согласно Федеральному закону №125-ФЗ «Об архивном деле в Российской Федерации» и иным нормативно правовым актам в области архивного дела и архивного хранения.

7. Согласие может быть отозвано субъектом персональных данных или его представителем путем направления письменного заявления Обществу или его представителю по адресу, указанному в начале данного Согласия.

8. В случае отзыва субъектом персональных данных или его представителем согласия на обработку персональных данных Общество вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 – 11 части 1 статьи 6, части 2

ООО «Коннект Лайн»
115280, РФ, г. Москва, вн.тер.г. муниципальный округ Даниловский
ул.Ленинская слобода, дом 19, оф.2031, ком.09
ОГРН 1187746094381
ИНН 7704450680

статьи 10 и части 2 статьи 11 Федерального закона №152-ФЗ «О персональных данных» от 27.07.2006 г.

9. Настоящее согласие действует все время до момента прекращения обработки персональных данных, указанных в п.7 и п.8 данного Согласия.