УТВЕРЖДАЮ
ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
ООО «УПРАВЛЕНИЕ
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ»

_____ М.А. Солдатов
«08» февраля 2019 г.

ПОЛИТИКА
безопасности персональных данных

1. Общая часть

1.1 Настоящая Политика определяет порядок создания, обработки и защиты персональных данных иных лиц, работников ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» (далее - организация).

1.2 Основанием для разработки данного локального нормативного акта являются:

- Конституция РФ от 12 декабря 1993 г. (ст. ст. 2, 17-24, 41);
- глава 14 (ст. 86-90) Трудового кодекса РФ;
- часть 1 и 2, часть 4 Гражданского кодекса РФ;
- Федеральный закон Российской Федерации от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон Российской Федерации от 29 декабря 2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Регламентирующие документы ФСТЭК России об обеспечении безопасности персональных данных:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15 февраля 2008 г.);

- Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Устав ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

1.3 Целью настоящей Политики является определение порядка обработки персональных данных иных лиц организации, лиц, работающих по трудовым договорам и гражданско-правовым договорам (далее – работников организации), согласно Перечню персональных данных, утвержденный Приказом руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ», обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным иных лиц, работников организации, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

2. Основные понятия, используемые в настоящей Политике

Для целей настоящей Политики применяются следующие термины и определения:

Оператор - юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Работники (субъекты персональных данных) - физические лица, состоящие или готовящиеся вступить в трудовые и иные гражданско-правовые отношения с организацией.

Документы, содержащие персональные данные иных лиц - документы, необходимые для осуществления действий в связи с обращением в организации, либо документы, содержащие сведения, предназначенные для использования в целях, предусмотренных Уставом организации.

Документы, содержащие персональные данные сотрудника – документы, которые сотрудник организации предоставляет организации, связанные с трудоустройством, работой и увольнением, а также с определением правового положения (статуса) сотрудника.

Документы, содержащие персональные данные работника - документы, которые работник предоставляет организации (работодателю) в связи с трудовыми отношениями и касающиеся конкретного работника (субъекта персональных данных), а также другие документы, содержащие сведения, предназначенные для использования в служебных целях.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, (обновление, накопление, хранение, уточнение изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных иного лица, работника.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в

информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной системы техники.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами 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.

3. Общие принципы обработки персональных данных иных лиц, работников

3.1 Обработка персональных данных иных лиц и работников осуществляется на основе принципов:

1) Обработка персональных данных должна осуществляться на законной и справедливой основе.

2) Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

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

5) Содержание и объем обрабатываемых персональных данных должны

соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

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

7) Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом № 152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральными законами.

3.2 В целях обеспечения прав и свобод человека и гражданина, Организация при обработке персональных данных иного лица, работника обязаны соблюдать следующие общие требования:

1) Обработка персональных данных иных лиц может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов; реализации приоритетов государственной политики, в соответствии с законодательством Российской Федерации.

2) Обработка персональных данных сотрудника организации осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, Федерального закона № 79-ФЗ, законодательства Российской Федерации в области персональных данных, других федеральных законов и иных нормативных правовых актов Российской Федерации, содействия сотруднику организации в работе, должностном росте, обеспечения личной безопасности сотрудника и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества, учета результатов исполнения им должностных обязанностей и обеспечения сохранности имущества организации.

3) Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, продвижении по службе, обеспечения личной безопасности работников,

контроля за количеством и качеством выполняемой работы и обеспечением сохранности имущества.

4) Все персональные данные иного лица следует получать у него самого. Все персональные данные работника работодатель должен получать у него самого. Если персональные данные иного лица, работника, возможно, получить только у третьей стороны, то иное лицо, работник должны быть уведомлены об этом заранее и от них должны быть получены письменные согласия.

5) При определении объема и содержания, обрабатываемых персональных данных иного лица, или работника, организация должна руководствоваться Конституцией Российской Федерации, Трудовым кодексом, законодательством РФ в сфере защиты персональных данных и обработки информации, Уставом организации и иными Федеральными законами, и локальными нормативными актами в области защиты персональных данных.

6) Организация не имеет права получать и обрабатывать персональные данные иного лица, сотрудника или работника, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ и другими федеральными законами.

7) Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении иного лица, сотрудника и работника или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

8) Решение, порождающее юридические последствия в отношении иного лица или работника, или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме иного лица и работника, или в случаях, предусмотренных Федеральным законодательством, устанавливающим также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

9) Организация (работодатель) обязан(а) разъяснить иному лицу и работнику порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные

юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты иным лицом и работником своих прав и законных интересов.

10) Организация обязана рассмотреть возражение в течение тридцати дней со дня его получения и уведомить иное лицо и работника о результатах рассмотрения такого возражения.

11) Защита персональных данных иных лиц, работников от неправомерного их использования или утраты должна быть обеспечена организацией за счет своих средств, в порядке, установленном федеральными законами.

12) Работники или их представители должны быть ознакомлены под личную подпись с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.3 Организация вправе поручить обработку персональных данных другому лицу с согласия иного лица, если иное не предусмотрено Федеральным законом № 152-ФЗ, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо путем принятия организацией соответствующего акта (далее - поручение организации). Лицо, осуществляющее обработку персональных данных по поручению организации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ. В поручении организации должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ.

3.4 В случае предусмотренном обработку персональных данных по поручению организации, не обязано получать согласие иного лица на обработку его персональных данных.

3.5 В случае если организация поручает обработку персональных данных другому лицу, ответственность перед иным лицом за действия указанного лица несет организация. Лицо, осуществляющее обработку персональных данных по поручению организации, несет ответственность перед организацией.

4. Получение персональных данных иного лица, сотрудника и работника

4.1 Получение персональных данных осуществляется путем представления их самим иным лицом, сотрудником или работником, на основании его письменного согласия, за исключением случаев прямо предусмотренных действующим законодательством Российской Федерации.

В случаях, предусмотренных федеральными законами, обработка персональных данных осуществляется только с согласия иного лица, сотрудником и работника в письменной форме. Равнозначным содержащему собственноручную подпись иного лица, сотрудника и работника согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом № 152-ФЗ электронной подписью. Согласие иного лица и работника в письменной форме на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование и адрес организации, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению организации если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых организацией способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено Федеральным законодательством;

9) подпись субъекта персональных данных.

В случае недееспособности иного лица согласие на обработку его персональных данных дает в письменной форме его законный представитель.

4.2 Сотрудник организации обязан:

- передавать организации комплекс достоверных документированных персональных данных, указанных в пункте 4.1 настоящего Положения;
- своевременно в срок, сообщать организации об изменении своих персональных данных.

4.3 В случае необходимости проверки персональных данных иного лица или работника заблаговременно должно сообщить об этом иному лицу или работнику, о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа иного лица или работника дать письменное согласие на их получение.

4.4 Обработка персональных данных работника не требует получения соответствующего согласия в следующих случаях:

1) Если объем обрабатываемых работодателем (представителем нанимателя) персональных данных не превышает установленные перечни, а также соответствует целям обработки, предусмотренным трудовым законодательством.

2) Обязанность по обработке, в том числе опубликованию и размещению персональных данных сотрудника в сети Интернет, предусмотрена законодательством Российской Федерации.

3) Обработка персональных данных близких родственников работника в объеме, предусмотренном унифицированной формой № Т-2, утвержденной постановлением Госкомстата Российской Федерации от 05 января 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат). В иных случаях, получение согласия близких родственников работника является обязательным условием обработки их персональных данных.

4) Обработка персональных данных близких родственников сотрудника организации в объеме, предусмотренном унифицированной формой № Т-2ГС, утвержденной постановлением Госкомстата Российской Федерации от 05 января 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в

случаях, установленных законодательством Российской Федерации (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат). В иных случаях, получение согласия близких родственников сотрудника организации является обязательным условием обработки их персональных данных.

5) Обработка специальных категорий персональных данных работника, в том числе, сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения работником трудовой функции на основании положений п. 2.3 ч. 2 ст. 10 Федерального закона «О персональных данных» в рамках трудового законодательства.

6) Обработка специальных категорий персональных данных сотрудника организации, в том числе, сведений о состоянии здоровья, относящихся к вопросу о возможности исполнения должностных обязанностей сотрудника организации.

7) При передаче персональных данных работника третьим лицам в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

8) При передаче персональных данных сотрудника организации третьим лицам в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника организации, а также в других случаях, предусмотренных федеральными законами.

9) При передаче его персональных данных в случаях, связанных с выполнением им должностных обязанностей, в том числе, при его командировании (в соответствии с Правилами оказания гостиничных услуг в Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 25 апреля 1997 г. № 490, нормативными правовыми актами в сфере транспортной безопасности).

10) В случаях передачи работодателем (представителем нанимателя) персональных данных работников в налоговые органы, военные комиссариаты, профсоюзные органы, предусмотренные действующим законодательством Российской Федерации.

11) При мотивированных запросах от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченных запрашивать информацию о работниках в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

В случае поступления запросов из организаций, не обладающих соответствующими полномочиями, работодатель (представитель нанимателя) обязан получить согласие работника на предоставление его персональных данных и предупредить лиц, получающих персональные данные работника, сотрудника о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что это правило будет (было) соблюдено.

12) Передача персональных данных работника, сотрудника кредитным организациям, открывающим и обслуживающим платежные карты для начисления заработной платы (денежного содержания), осуществляется без его согласия в следующих случаях:

- договор на выпуск банковской карты заключался напрямую с работником, сотрудником и в тексте, которого предусмотрены положения, предусматривающие передачу работодателем (представителем нанимателя) персональных данных работника, сотрудника;
- наличие у работодателя (представителя нанимателя) доверенности на представление интересов работника, сотрудника при заключении договора с кредитной организацией на выпуск банковской карты и ее последующем обслуживании;

13) Обработка персональных данных работника, сотрудника при осуществлении пропускного режима на территорию служебных зданий и помещений работодателя (представителя нанимателя), при условии, что организация пропускного режима осуществляется работодателем (представителем нанимателя) самостоятельно.

4.5 Обработка персональных данных соискателей на замещение вакантных должностей в рамках правоотношений, урегулированных Трудовым кодексом РФ, предполагает получение согласия соискателей на замещение вакантных должностей на обработку их персональных данных на период принятия работодателем решения о приеме либо отказе в приеме на работу.

Исключение составляют случаи, когда от имени соискателя действует кадровое агентство, с которым данное лицо заключил соответствующий договор, а также при самостоятельном размещении соискателем своего резюме в сети Интернет, доступного неограниченному кругу лиц.

При поступлении в адрес работодателя резюме, составленного в произвольной форме, при которой однозначно определить физическое лицо, его направившее не представляется возможным, данное резюме подлежит уничтожению в день поступления.

В случае, если сбор персональных данных соискателей осуществляется посредством типовой формы анкеты соискателя, утвержденной оператором, то данная типовая форма анкеты должна соответствовать требованиям п. 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687, а также содержать информацию о сроке ее рассмотрения и принятия решения о приеме либо отказе в приеме на работу.

Типовая форма анкеты соискателя может быть реализована в электронной форме на сайте организации, где согласие на обработку персональных данных подтверждается соискателем путем проставления отметки в соответствующем поле, за исключением случаев, когда работодателем запрашиваются сведения, предполагающие получение согласия в письменной форме.

В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней.

Получение согласия также является обязательным условием при направлении работодателем запросов в иные организации, в том числе, по прежним местам работы, для уточнения или получения дополнительной информации о соискателе.

5. Хранение и использование персональных данных иных лиц, сотрудников и работников

5.1 Информация персонального характера иного лица и работника хранится и обрабатывается с соблюдением требований действующего Российского законодательства о защите персональных данных.

5.2 Порядок хранения документов, содержащих персональные данные работников осуществлять в соответствии с:

- Правилами, устанавливающими порядок ведения и хранения трудовых книжек, а также порядок изготовления бланков трудовой книжки и обеспечения ими работодателей, утвержденными Постановлением Правительства РФ от 16 апреля 2003 г. № 225 «О трудовых книжках»;
- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных

данных».

5.3 Обработка персональных данных иных лиц, работников организации осуществляется смешанным путем:

- неавтоматизированным способом обработки персональных данных;

- автоматизированным способом обработки персональных данных (с помощью ПЭВМ и специальных программных продуктов).

5.4 Персональные данные иных лиц, работников хранятся на бумажных носителях и в электронном виде.

5.5 Хранение текущей документации и оконченной производством документации, содержащей персональные данные иных лиц, работников организации, осуществляется во внутренних подразделениях организации, а также в помещениях организации, предназначенных для хранения отработанной документации, в соответствии с действующим Приказом руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» .

Ответственные лица за хранение документов, содержащих персональные данные иных лиц, работников, назначены Приказом организации.

5.6 Хранение персональных данных иных лиц, работников осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Хранение документов, содержащих персональные данные иных лиц, работников, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению.

5.7 Организация обеспечивает ограничение доступа к персональным данным иных лиц, работников лицам, не уполномоченным федеральными законами, либо образовательным учреждением для получения соответствующих сведений.

5.8 Доступ к персональным данным иных лиц, работников без специального разрешения имеют только должностные лица организации, допущенные к работе с персональными данными иных лиц, работников Приказом руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» . Данным категориям работников в их должностные обязанности включается пункт об обязанности соблюдения требований по защите персональных данных.

1. Защита персональных данных иных лиц, сотрудников и работников

6.1 Организация при обработке персональных данных иных лиц, работников обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.2 Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

6.3 Обеспечение безопасности персональных данных иных лиц, работников достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем над принимаемыми мерами по обеспечению безопасности

персональных данных и уровня защищенности информационных систем персональных данных.

6.4 Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона «О персональных данных».

6.5 Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

6.6 Для обеспечения безопасности персональных данных иных лиц, работников при неавтоматизированной обработке предпринимаются следующие меры:

6.6.1 Определяются места хранения персональных данных, которые оснащаются средствами защиты:

- В кабинетах, где осуществляется хранение документов, содержащих персональные данные иных лиц, работников, имеются сейфы, шкафы, стеллажи, тумбы.

- Дополнительно кабинеты, где осуществляется хранение документов, оборудованы замками и системами охранной (пультовой) и пожарной сигнализаций.

- Организация использует услуги вневедомственной охраны.

- В здании, где расположена организация, имеется пропускная система.

6.6.2 Все действия по неавтоматизированной обработке персональных данных иных лиц, работников осуществляются только должностными лицами, согласно Списку должностей, утвержденному Приказом руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ», и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

6.6.3 При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие

меры:

1) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) только копия;

2) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление).

Персональные данные иных лиц, работников, содержащиеся на материальных носителях, уничтожаются по Акту об уничтожении персональных данных.

Эти правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

6.6.4 Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.7 Для обеспечения безопасности персональных данных иного лица,

работника при автоматизированной обработке предпринимаются следующие меры:

6.7.1 Все действия при автоматизированной обработке персональных данных иных лиц, работников осуществляются только должностными лицами, согласно Списку должностей, утвержденному Приказом руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ», и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

6.7.2 Персональные компьютеры, имеющие доступ к базам хранения персональных данных иных лиц, работников, защищены паролями доступа. Пароли устанавливаются Администратором информационной безопасности и сообщаются индивидуально работнику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных иных лиц, работников на данном ПК.

6.7.3 Иные меры, предусмотренные Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

6.8 Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с приказами по архивному делу, или продлевается на основании заключения экспертной комиссии организации, если иное не определено законодательством РФ.

7. Передача персональных данных иных лиц, сотрудников и работников третьим лицам

7.1 Передача персональных данных иных лиц третьим лицам осуществляется организацией только с письменного согласия иного лица, с подтверждающей визой руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ», за исключением случаев, если:

1) передача необходима для защиты жизни и здоровья иного лица, либо других лиц, и получение его согласия невозможно;

2) по запросу органов дознания, следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством, в соответствии с Законом об оперативно-розыскной деятельности;

3) при наличии оснований, позволяющих полагать, что права и интересы иного лица могут быть нарушены противоправными действиями других лиц;

4) в иных случаях, прямо предусмотренных Федеральным

законодательством.

Лица, которым в установленном Федеральным законом №152-ФЗ порядке переданы сведения, составляющие персональные данные иного лица, несут дисциплинарную, административную или уголовную ответственность за разглашение в соответствии с законодательством Российской Федерации.

7.2 Передача персональных данных иного лица третьим лицам осуществляется на основании запроса третьего лица с разрешающей визой руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» при условии соблюдения требований, предусмотренных п. 7.1 настоящей Политики.

7.3 При передаче персональных данных работника третьим лицам работодатель должен соблюдать следующие требования:

7.3.1 Не сообщать персональные данные работника, третьему лицу без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, прямо предусмотренных федеральными законами.

7.3.2 Не сообщать персональные данные работника, в коммерческих целях без его письменного согласия.

7.3.3 Предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

7.3.4 Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником, трудовой функции (должностных обязанностей).

7.3.5 Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом РФ, и только в том объеме, который необходим для выполнения указанными представителями их функций.

7.4 Передача персональных данных работника, третьим лицам осуществляется на основании письменного заявления/запроса третьего лица с разрешающей визой руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» и только с согласия работника, в отношении которого поступил такой запрос, за исключением случаев, прямо предусмотренных п. 7.3.1 настоящей Политики.

7.5 Получателями персональных данных работников, могут относиться организации, в т.ч. государственные учреждения, органы государственной власти, получающие персональные данные в объеме и в порядке, определенном действующим законодательством, а именно:

- налоговые органы;
- правоохранительные органы;
- судебные органы;
- органы статистики;
- военкоматы;
- органы социального страхования (медицинские страховые организации в соответствии с договором обязательного медицинского страхования работающих граждан);
- банковские организации;
- пенсионные фонды;
- подразделения муниципальных органов управления;
- другие получатели, в том числе вышестоящие федеральные органы исполнительной власти (по подведомственности).

Организация обеспечивает ведение Журнала учета выданных персональных данных иных лиц, работников по запросам третьих лиц, в котором регистрируются поступившие запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных, а также отмечается, какая именно информация была передана.

В случае если лицо, обратившееся с запросом, не уполномочено федеральными законами на получение персональных данных иного лица, работника, либо отсутствует письменное согласие иного лица, работника на передачу его персональных данных, организация обязана отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, выдается мотивированный отказ в предоставлении персональных данных в письменной форме, копия отказа хранится в организации.

8. Права и обязанности иного лица, сотрудника и работника в области защиты его персональных данных

8.1. В целях обеспечения защиты персональных данных, хранящихся в организации, иные лица имеют право на:

- полную информацию о составе и содержимом их персональных данных, а также способе обработки этих данных;
- свободный доступ к своим персональным данным.

Иное лицо имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных организации;
2) правовые основания и цели обработки персональных данных;

3) цели и применяемые организации способы обработки персональных данных;

4) наименование и место нахождения организации, сведения о лицах (за исключением работников организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с организацией или на основании Федерального закона № 152-ФЗ;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению организации, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или Федеральным законодательством.

Сведения должны быть предоставлены иному лицу организации в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Сведения предоставляются иному лицу или его представителю организации при обращении, либо при получении запроса иного лица или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность иного лица или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие иного лица в отношениях с организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных организации, подпись иного лица или его представителя. Запрос может быть направлен в форме электронного

документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

В случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления иному лицу по его запросу, иное лицо вправе обратиться повторно в организацию или направить ему повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законодательством, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Иное лицо вправе требовать от организации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

8.2. В случае выявления неправомерной обработки персональных данных при обращении иного лица или его представителя либо по запросу иного лица или его представителя либо уполномоченного органа по защите прав субъектов персональных данных организации обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению организации) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении иного лица или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных организации обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению организации) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы иного лица или третьих лиц.

8.3. В случае подтверждения факта неточности персональных данных организации на основании сведений, представленных иным лицом или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению организации в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

8.4. В случае выявления неправомерной обработки персональных данных, осуществляемой организацией (или лицом, действующим по поручению организации), Организация в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению организации. В случае если обеспечить правомерность обработки персональных данных невозможно, организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных организация обязана уведомить иное лицо или его представителя, а в случае, если обращение иного лица или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

8.5. В случае достижения цели обработки персональных данных организация обязана прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению организации) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению организации) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является иное лицо, иным соглашением между организацией

и иным лицом, либо если организация не вправе осуществлять обработку персональных данных без согласия иного лица на основаниях, предусмотренных Федеральным законом № 152-ФЗ или Федеральным законодательством.

8.6. В случае отзыва иным лицом согласия на обработку его персональных данных организация обязана прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению организации) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению организации) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между организацией и иным лицом, либо если организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или Федеральным законодательством.

8.7. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, организация осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению организации) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен Федеральным законодательством.

8.8. Для своевременной и полной реализации своих прав, иное лицо обязано предоставить организации достоверные персональные данные.

8.9. Работник:

8.9.1. При приеме на работу предоставляет работодателю (представителю нанимателя) свои полные и достоверные персональные данные.

8.9.2. Для своевременной и полной реализации своих трудовых, пенсионных и иных прав работник обязуется поставить в известность работодателя об изменении персональных данных, обрабатываемых работодателем в связи с трудовыми отношениями,

в том числе изменении фамилии, имени, отчества, паспортных данных, о получении образования, квалификации, получении инвалидности и иных медицинских заключений, препятствующих выполнению своих должностных обязанностей.

8.2. **В целях обеспечения защиты персональных данных работник, имеет право на:**

8.2.1.1. Полную информацию о хранящихся у работодателя (представителя нанимателя) его персональных данных.

8.2.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника за исключением случаев, предусмотренных федеральными законами.

Выдача документов, содержащих персональные данные работников, осуществляется в соответствии со ст. 62 Трудового кодекса Российской Федерации, гл. 3 ст. 14 Федерального закона № 152-ФЗ с соблюдением следующей процедуры:

- заявление работника о выдаче того или иного документа на имя руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» (работодателя/представителя нанимателя);
- выдача заверенной копии (в количестве экземпляров, необходимом работнику) заявленного документа либо справки о заявленном документе или сведениях, содержащихся в нем;
- внесение соответствующих записей в журнал учета выданной информации.

8.10.3 Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением. При отказе работодателя (представителя нанимателя) исключить или исправить персональные данные работника, он имеет право заявить в письменной форме работодателю (представителю нанимателя) о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

8.10.4 Требование об извещении работодателем (представителем нанимателя) всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника обо всех произведенных в них исключениях, исправлениях или дополнениях.

8.10.5 Обжалование в суд любых неправомерных действий или бездействия

работодателя (представителя нанимателя) при обработке и защите его персональных данных.

8.10.6 Иные права, предусмотренные действующим законодательством.

8.3. **Работодатель обязан:**

8.11.1 Предоставить работнику по его просьбе информацию о наличии у него персональных данных владельца, цели их обработки, способ обработки, разъяснить юридические последствия отказа работника от их предоставления в случае, если такая обязанность предусмотрена федеральными законами.

8.11.2 По письменному заявлению работника не позднее 3-х рабочих дней со дня его подачи бесплатно выдавать работнику копии документов, связанных с работой.

8.11.3 Устранять выявленные недостоверные персональные данные в случаях и порядке, предусмотренном федеральными законами.

8.11.4 Принимать необходимые меры по обеспечению безопасности персональных данных работников при их обработке.

8.12 **Работодатель имеет право:**

8.12.1 Запросить от работника предоставления персональных данных и документов, их подтверждающих, в случаях, предусмотренных Федеральным законодательством.

8.12.2 Иные права, предусмотренные действующим законодательством.

9. Право на обжалование действий или бездействия организации

9.1 Если работник организации считает, что организация осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

9.2 Иное лицо, работник организации имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных иных лиц, сотрудников и работников

10.1 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных иного лица, работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральным законодательством.

10.2 Сотрудники организации, допущенные к обработке персональных данных иных лиц, работников, за разглашение полученной в ходе своей трудовой деятельности информации, несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

10.3 Моральный вред, причиненный иному лицу, работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

11. Заключительные положения

11.1 Настоящая Политика вступает в силу с даты его утверждения.

11.2 При необходимости приведения настоящей Политики в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании Приказа руководителя ООО «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» .

11.3 Настоящая Политика распространяется на всех работников, а также сотрудников организации, имеющих доступ и осуществляющих перечень действий с персональными данными иных лиц, работников.

11.4 Иные лица организации, а также их законные представители имеют право, ознакомится с настоящей Политикой.

11.5 В обязанности работников, осуществляющих первичный сбор персональных данных иного лица, входит получение согласия иного лица на обработку его персональных данных под личную подпись.

11.6 В обязанности работодателя входит ознакомление всех работников с настоящей Политикой и лиц, принимаемых на работу до подписания трудового договора, под личную подпись.

11.7 В обязанности представителя нанимателя входит ознакомление всех сотрудников организации с настоящим документом.

11.8 Документы, определяющие политику в отношении обработки персональных данных иных лиц, работников, размещены на официальном сайте или информационном стенде организации в течение 10 дней после их утверждения.