

УТВЕРЖДАЮ

Ректор ФГБОУ ВО «ИГУ»

Аргучинцев А.В.

«01» марта 2016г.



**ПОЛОЖЕНИЕ О ПЕРСОНАЛЬНЫХ ДАННЫХ
ФГБОУ ВО «ИГУ»**

Иркутск, 2016

ОГЛАВЛЕНИЕ

I. ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ФГБОУ ВО «ИГУ»	2
II. ПОЛОЖЕНИЕ О ПЕРСОНАЛЬНЫХ ДАННЫХ АБИТУРИЕНТОВ И ОБУЧАЮЩИХСЯ ФГБОУ ВО «ИГУ».....	14
III. ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНТРАГЕНТОВ ФГБОУ ВО «ИГУ».....	24
IV. ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИХ ЛИЦ	29
V. ПОЛОЖЕНИЕ О НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ФГБОУ ВО «ИГУ».....	33
VI. ПОЛОЖЕНИЕ О МЕРАХ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФГБОУ ВО «ИГУ»	38
VII. НОРМАТИВНЫЕ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ.....	44

I. ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ ФГБОУ ВО «ИГУ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящим Положением об обработке и защите персональных данных Работников (далее – Положение) устанавливается порядок обработки персональных данных Работников ФГБОУ ВО «ИГУ» (далее – Университет или Работодатель) и гарантии конфиденциальности сведений, предоставляемых Работником Работодателю.

1.2. Работниками являются физические лица (субъекты персональных данных), заключившие с Работодателем трудовые договоры.

1.3. Обработка персональных данных Работников в Университете заключается в сборе, записи, систематизации, накоплении, хранении, уточнении (обновлении, изменении), извлечении, использовании, передаче (распространении, предоставлении, доступе), обезличивании, блокировании, удалении, уничтожении и в защите от несанкционированного доступа к персональным данным.

1.4. Настоящее Положение и изменения к нему утверждаются ректором Университета и вводятся в действие приказом по основной деятельности Университета. Все Работники Университета должны быть ознакомлены под подпись с данным Положением и изменениями к нему.

1.5. Настоящее Положение является обязательным для исполнения всеми Работниками Университета, имеющими доступ к персональным данным Работников.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Под персональными данными Работников понимается информация, необходимая Работодателю в связи с трудовыми отношениями и касающаяся конкретного Работника, а также сведения о фактах, событиях и обстоятельствах жизни Работника, позволяющие идентифицировать его личность.

2.2. Персональные данные Работника, обработка которых осуществляется в Университете, включают следующие документы и сведения:

- фамилия, имя, отчество;
- фамилия при рождении (либо другие фамилии, если они были);
- день, месяц, год и место рождения;
- паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ);
- гражданство;
- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства;
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);
- копии документов об образовании;
- сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения,

квалификация и специальность по окончании образовательного учреждения и иные сведения;

- копии документов о повышении квалификации;
- сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса и телефона работодателя, а также реквизитов иных организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также иные сведения);
- 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 дата изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- вторые экземпляры трудового договора с Работниками;
- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- трудовые книжки и вкладыши к ним;
- карточки унифицированной формы Т-2 «Личная карточка работника»;
- личные дела Работников в бумажной форме;
- фотографическое изображение работника;
- сведения о заработной плате (номера счетов для расчета с Работниками, в том числе номера их банковских карточек);
- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и иные сведения);
- копии военных билетов;
- сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и) или иных членов семьи, паспортные данные супруга(и) или иных членов семьи (паспортные данные или данные свидетельства о рождении), данные справки по форме 2НДФЛ супруга(и) или иных членов семьи);
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;
- сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования);
- сведения, указанные в оригиналах и копиях приказов по персоналу Университета и материалах к ним, в том числе информация об отпусках, о командировках и т.п.;
- оригиналы приказов, изданных в Университете, и относящиеся к субъекту персональных данных, и материалы к данным приказам;
- сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) Работников Университета;
- материалы по аттестации и оценке Работников Университета;
- материалы по внутренним служебным расследованиям в отношении Работников Университета;
- сведения о временной нетрудоспособности Работников Университета;

- табельный номер Работника Университета;
- сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и иные сведения);
- иные сведения, с которыми Работник считает нужным ознакомить Работодателя.

3. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Документы, перечисленные в п.2.2. Положения, содержащие сведения о персональных данных Работников Университета, являются конфиденциальными. Университет обеспечивает конфиденциальность персональных данных, и обязан не допускать их распространения без согласия Работника, либо наличия иного законного основания.

3.2. Все меры конфиденциальности при сборе, обработке и хранении персональных данных Работников распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

4. ПРАВА И ОБЯЗАННОСТИ РАБОТОДАТЕЛЯ

4.1. Работодатель имеет право без согласия Работника осуществлять обработку его персональных данных в следующих случаях:

4.1.1. если обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации и в целях исполнения трудового договора с Работником;

4.1.2. если обработка персональных данных Работника осуществляется для статистических или иных научных целей при условии обязательного обезличивания его персональных данных;

4.1.3. если обработка персональных данных Работника необходима для защиты жизни, здоровья или иных жизненно важных интересов Работника, если получение его согласия невозможно.

4.1.4. в случаях, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

4.1.5. В иных случаях (не поименованных в п.4.1. Положения) Работодатель может осуществлять обработку персональных данных Работника только с письменного согласия Работника. Согласие на обработку персональных данных по основаниям данного пункта может быть отозвано Работником. Обязанность предоставить доказательство получения согласия Работника на обработку его персональных данных по основаниям данного пункта, возлагается на Работодателя.

4.2. Письменное согласие Работника на обработку своих персональных данных по основаниям пп.4.1.1. Положения должно включать в себя:

- фамилию, имя, отчество, адрес Работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Работодателя, получающего согласие Работника;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие Работник;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Работодателем способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва;
- личную подпись Работника.

4.3. В целях обеспечения прав и свобод человека и гражданина Работодатель и его представители при обработке персональных данных Работника обязаны соблюдать следующие общие требования:

- Обработка персональных данных Работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия Работникам в трудоустройстве, обучения и продвижении в Университете, обеспечения

личной безопасности Работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

- При определении объема и содержания персональных данных Работника, подлежащих обработке, Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и иными федеральными законами.

4.4. Работодатель не имеет права получать и обрабатывать персональные данные Работника 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 Работодатель вправе получать и обрабатывать данные о частной жизни Работника только с его письменного согласия.

4.5. Работодатель не имеет права получать и обрабатывать персональные данные Работника о его членстве в организациях или его профсоюзной деятельности, за исключением случаев, предусмотренных действующим законодательством.

4.6. Работодатель не должен запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Работником трудовой функции.

4.7. При принятии решений, затрагивающих интересы Работника, Работодатель не имеет права основываться на персональных данных Работника, полученных исключительно в результате их автоматизированной обработки.

4.8. Защита персональных данных Работника от неправомерного их использования или утраты должна быть обеспечена Работодателем за счет средств Университета в порядке, установленном федеральным законодательством.

5. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА

5.1. Работник обязан передавать Работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации, настоящим Положением и Правилами внутреннего трудового распорядка, принятыми в Университете.

5.2. Работник должен своевременно в срок, не превышающий пяти рабочих дней, сообщать Работодателю об изменении своих персональных данных.

5.3. В целях обеспечения защиты персональных данных, хранящихся у Работодателя, Работник имеет право:

5.3.1. На полную информацию о своих персональных данных и обработке этих данных; на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Работника, за исключением случаев, предусмотренных федеральным законом.

Сведения о наличии персональных данных должны быть предоставлены Работнику в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

5.3.2. Определить своих представителей для защиты своих персональных данных.

5.3.3. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона.

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

5.5. При отказе Работодателя исключить или исправить персональные данные Работника последний имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия;

Персональные данные оценочного характера Работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.6. Требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.7. Обжаловать в суде любые неправомерные действия или бездействие Работодателя при обработке и защите его персональных данных.

5.8. Передача информации третьей стороне возможна только при письменном согласии Работника, за исключением обстоятельств, установленных законодательством.

5.9. Если Работник считает, что Работодатель осуществляет обработку его персональных данных с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, Работник вправе обжаловать действия или бездействие Работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

5.10. Работник имеет право на сохранение и защиту своей личной и семейной тайны, на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5.11. Во всех случаях отказ Работника от своих прав на сохранение и защиту конфиденциальности его персональных данных недействителен и юридически ничтожен.

6. СБОР И ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Сбор персональных данных

– все персональные данные Работника Работодатель получает у него самого;

– если персональные данные Работника возможно получить только у третьей стороны, то Работник уведомляется об этом Работодателем заранее. Работодателем в этом случае должно быть получено письменное согласие Работника. Работодатель должен сообщить Работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и о последствиях отказа Работника дать письменное согласие на их получение;

– работник Университета предоставляет работнику управления кадров достоверные сведения о себе. Информация, представляемая Работником при поступлении на работу в Университет, должна иметь документальную форму. Работник управления кадров Университета проверяет достоверность сведений, сверяя данные, предоставленные Работником, с имеющимися у Работника документами.

6.2. При заключении трудового договора в соответствии со ст.65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет Работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или Работник поступает на работу на условиях совместительства, либо трудовая книжка у Работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета — для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний — при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника);
- справку о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям.

6.3. Документы, содержащие персональные данные Работника, создаются путём:

- создания комплекта документов, сопровождающих процесс оформления трудовых отношений Работника в Университете при его приеме, переводе и увольнении методом внесения сведений в учётные формы (на бумажных и электронных носителях);
- копирования оригиналов документов (документ об образовании, свидетельство ИНН, пенсионное свидетельство);
- получения оригиналов необходимых документов (трудовая книжка, личный листок по учёту кадров, автобиография).

6.4. При поступлении на работу в Университет:

- Работником управления кадров заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные Работника:
 - общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные, сведения о месте жительства и контактных телефонах);
 - сведения о воинском учете;
 - данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения об изменении места жительства, контактных телефонов.

6.5. Личное дело Работника оформляется после издания приказа о приеме на работу.

- Все документы личного дела подшиваются в обложку образца, установленного в Университете. На ней указываются фамилия, имя отчество Работника, номер личного дела. К каждому личному делу прилагается фотография Работника размером 3х4.

- Все документы, поступающие в личное дело, располагаются в хронологическом порядке. Листы документов, подшитые в личное дело, нумеруются.

- Личное дело ведется на протяжении всей трудовой деятельности Работника в Университете. Изменения, вносимые в личное дело, должны быть подтверждены соответствующими документами.

6.6. Хранение персональных данных

6.6.1. Персональные данные Работников могут храниться, как на бумажных носителях, так и в электронном виде.

6.6.2. В управлении кадров Университета хранятся в специально отведенных системах хранения (шкафах, сейфах) следующие группы документов, содержащие данные Работников в единичном или сводном виде:

- документы, содержащие персональные данные Работников (комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекты документов по тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Университета, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие ведомства.
- документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции Работников, приказы, распоряжения, указания руководства Университета); документы по планированию, учету, анализу и отчетности в части работы с персоналом Университета.

6.6.3. В том числе в специально отведенных системах хранения (шкафах, сейфах) согласно приказу, определяющему места хранения носителей персональных данных, хранятся:

- трудовые книжки, личные карточки Работников по форме Т-2;

- личные дела в бумажном виде в папках, прошитые и пронумерованные по страницам.

Личные дела находятся в управлении кадров.

6.6.4. Ключи от шкафов, сейфов хранятся лично у начальника Управления кадров и ректора Университета.

6.7. Персональные данные Работников могут также храниться в электронном виде в информационных системах персональных данных Университета, в электронных папках и файлах в ПК работников Университета: начальника управления кадров, работников управления кадров, главного бухгалтера и работников управления бухгалтерского учета и контроля, начальника и работников ФЭУ, начальника и работников юридического управления, начальника и работников Второго управления.

Доступ к ПК строго ограничен кругом лиц, определённых приказом ректора Университета.

6.8. Хранение персональных данных в управлении бухгалтерского учета и контроля:

- согласно приказу, определяющему места хранения носителей персональных данных, персональные данные, содержащиеся на бумажных носителях, хранятся в шкафах, сейфах, установленных в служебных помещениях, занимаемых главным бухгалтером и иными работниками управления бухгалтерского учета и контроля.
- персональные данные, содержащиеся на электронных носителях информации, хранятся согласно приказу, определяющему места хранения носителей персональных данных.

6.9. Обработка и хранение документов воинского учёта, содержащих персональные данные Работников, осуществляется во Втором управлении.

6.10. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

6.11. Персональные данные, содержащиеся на электронных носителях информации, уничтожаются по акту по истечению установленного срока хранения.

7. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. При передаче персональных данных Работника Работодатель должен соблюдать следующие требования:

- не сообщать персональные данные Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья Работника, а также в случаях, установленных федеральным законом;

- предупредить лиц, получающих персональные данные Работника 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;

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

- передавать персональные данные Работника представителям Работников в порядке, установленном Трудовым кодексом Российской Федерации и Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», и ограничивать эту информацию только теми персональными данными Работника, которые необходимы для выполнения указанными представителями их функций.

7.2. Передача персональных данных Работника третьим лицам осуществляется только с письменного согласия Работника, которое оформляется по установленной форме (Приложение №1) и должно включать в себя:

- фамилию, имя, отчество, адрес Работника, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Работодателя, получающего согласие Работника;
- цель передачи персональных данных;
- перечень персональных данных, на передачу которых дает согласие Работник;

- срок, в течение которого действует согласие, а также порядок его отзыва.

- Согласия Работника на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника; когда третьи лица оказывают услуги Работодателю на основании заключенных договоров, а также в случаях, установленных действующим законодательством и настоящим Положением.
- Работники Работодателя, передающие персональные данные Работников третьим лицам, должны передавать их с обязательным составлением акта приема-передачи документов (иных материальных носителей), содержащих персональные данные работников. Акт составляется по установленной форме (Приложение №3), и должен содержать следующие условия:

- уведомление лица, получающего данные документы об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена;

- предупреждение об ответственности за незаконное использование данной конфиденциальной информации в соответствии с федеральными законами.

7.2. Передача документов (иных материальных носителей), содержащих персональные данные Работников, осуществляется при наличии у лица, уполномоченного на их получение:

- договора на оказание услуг Университету;

- соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных Работника;

- письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные Работника, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных Работника Университета несет начальник управления кадров, а также работник, осуществляющий передачу персональных данных Работника третьим лицам.

7.3. Представителю Работника персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя Работника;

- письменного заявления Работника, написанного в присутствии работника управления кадров Работодателя (если заявление написано Работником не в присутствии работника управления кадров, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в отделе кадров в личном деле Работника.

7.4. Предоставление персональных данных Работника государственным органам производится в соответствии с требованиями действующего законодательства.

7.5. Персональные данные Работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Работника, за исключением случаев, когда передача персональных данных Работника без его согласия допускается действующим законодательством Российской Федерации.

7.6. Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии письменного согласия Работника, удостоверенного нотариально.

7.7. Документы, содержащие персональные данные Работника, могут быть отправлены через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

8. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКА

8.1. Право доступа к персональным данным Работника в Университете имеют:

- ректор;
- начальник и работники управления кадров;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным Работника может иметь руководитель нового подразделения;
- сам Работник – субъект персональных данных;
- другие работники Университета при выполнении ими своих служебных обязанностей.

8.2. Перечень работников Университета, имеющих доступ к персональным данным Работников, определяется приказом ректора Университета.

9. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

9.1. Университет обязан при обработке персональных данных принимать необходимые правовые, организационные и технические меры для защиты персональных данных Работников от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

9.2. Защите подлежит:

- информация о персональных данных Работника, содержащаяся на бумажных носителях;
- документы, содержащие персональные данные Работника;
- персональные данные, содержащиеся на электронных носителях.

9.3. Общую организацию защиты персональных данных Работников по указанию ректора осуществляет назначенный работник, ответственный за организацию обработки персональных данных, и начальник управления кадров в соответствии с должностными инструкциями.

9.4. Начальник управления кадров обеспечивает:

- Ознакомление работника под роспись с настоящим Положением.
- Истребование с работников письменного обязательства о соблюдении конфиденциальности персональных данных Работника и соблюдении правил их обработки.
- Ознакомление работника под роспись с приказами и иными внутренними локальными нормативными актами, регуливающими обработку и защиту персональных данных в Университете.
- Общий контроль соблюдения Работниками мер по защите персональных данных.

9.5. Защита информационных систем Университета, в которых обрабатываются персональные данные Работников, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке, осуществляется в соответствии с Положением о мерах по организации защиты информационных систем персональных данных Университета.

9.6. Доступ к персональным данным Работника имеют работники Работодателя, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей согласно перечню должностей.

В целях выполнения порученного задания и на основании служебной записки с положительной резолюцией ректора, доступ к персональным данным Работника может быть предоставлен иному работнику, должность которого не включена в Перечень должностей работников, имеющих доступ к персональным данным Работника Университета, и которым они необходимы в связи с исполнением трудовых обязанностей.

9.6.1. Все работники, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных Работников (соглашение о неразглашении конфиденциальной информации).

Процедура оформления доступа к персональным данным Работника включает в себя:

- ознакомление Работника под роспись с настоящим Положением. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и

защиту персональных данных Работника, с данными актами также производится ознакомление Работника под подпись.

- истребование с работника (за исключением ректора) письменного обязательства о соблюдении конфиденциальности персональных данных Работника и соблюдении правил их обработки, подготовленного по установленной форме.

9.6.2. Работник Работодателя, имеющий доступ к персональным данным Работников в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные Работника, исключая доступ к ним третьих лиц.

В отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные Работников.

- При уходе в отпуск, во время служебной командировки и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные Работников лицу, на которое локальным актом Университета (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные Работников, передаются другому работнику, имеющему доступ к персональным данным Работников по указанию руководителя структурного подразделения.

9.6.3. При увольнении работника, имеющего доступ к персональным данным Работников, документы и иные носители, содержащие персональные данные Работников, передаются другому работнику, имеющему доступ к персональным данным Работников по указанию руководителя структурного подразделения или ректора.

9.6.4. Допуск к персональным данным Работника других работников Работодателя, не имеющих надлежащим образом оформленного доступа, запрещается.

9.7. Личные дела и документы, содержащие персональные данные Работников, хранятся в запирающихся шкафах (сейфах), обеспечивающих защиту от несанкционированного доступа.

9.7.1. В Университете не допускается выдача личных дел работников на рабочие места руководителей. Личные дела могут выдаваться только ректору. В исключительных случаях, по письменному разрешению ректора, - руководителю структурного подразделения (например, при подготовке материалов для аттестации Работника).

9.7.2. В конце рабочего дня все личные дела, выданные работникам, имеющим право доступа к этим документам, сдаются в управление кадров.

9.8. Защита доступа к электронным носителям, содержащим персональные данные Работников, обеспечивается, том числе:

- использованием лицензированных антивирусных и антихакерских программ, не допускающих несанкционированный доступ к персональным данным;
- разграничением прав доступа с использованием учетной записи;
- 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;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
- контролем эффективности принимаемых мер по обеспечению защищенности персональных данных.

9.9. Копировать и делать выписки персональных данных Работника разрешается исключительно в служебных целях с письменного разрешения начальника управления кадров.

9.10. Ответы на письменные запросы других организаций и учреждений о персональных данных Работников Университета даются только с письменного согласия самого Работника, если иное не установлено законодательством. Ответы оформляются в письменном виде, на бланке Университета, и в том объеме, который позволяет не разглашать излишний объем персональных сведений о Работниках Университета.

9.11. Передача информации, содержащей сведения о персональных данных Работников Университета, по телефону, факсимильной связи, электронной почте запрещается.

10. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

10.1. Руководитель, разрешающий доступ работника к документам, содержащим персональные данные Работника, несет персональную ответственность за данное разрешение.

10.2. Каждый работник Университета, получающий для работы документ, содержащий персональные данные Работника, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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

10.4. За неисполнение или ненадлежащее исполнение Работником по его вине возложенных на него обязанностей по соблюдению установленного порядка обработки персональных данных Работников Работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.

10.4.1. К лицам, виновным в нарушении норм, регулирующих получение, обработку и защиту персональных данных Работника, могут быть применены следующие дисциплинарные взыскания:

- а) замечание;
- б) выговор;
- в) увольнение.

10.4.2. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

10.4.3. Приказ о применении к Работнику дисциплинарного взыскания с указанием оснований его применения объявляется Работнику под роспись в течение трех рабочих дней со дня его издания, не считая времени отсутствия работника на работе.

10.4.4. Если в течение года со дня применения дисциплинарного взыскания Работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с Работника по собственной инициативе, по письменному заявлению Работника или по ходатайству его непосредственного руководителя.

10.5. Должностные лица, в обязанность которых входит ведение персональных данных работника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

10.6. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на Работников.

10.7. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

11. СПИСОК ИСПОЛЬЗОВАННЫХ ЗАКОНОДАТЕЛЬНЫХ И НОРМАТИВНЫХ АКТОВ

Разработка настоящего Положения осуществлена в соответствии со следующими нормативными документами:

Конституция Российской Федерации (часть 1 статьи 23, статья 24);

Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ;

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

II. ПОЛОЖЕНИЕ О ПЕРСОНАЛЬНЫХ ДАННЫХ АБИТУРИЕНТОВ И ОБУЧАЮЩИХСЯ ФГБОУ ВО «ИГУ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого иного использования персональных данных абитуриентов, а также обучающихся по программам специалитета, бакалавриата, магистратуры, слушателей, аспирантов и докторантов (далее - обучающихся) федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский государственный университет» (далее - Университет), а также ведения их личных дел.

1.2 Цель настоящего Положения - защита персональных данных абитуриентов и обучающихся Университета от несанкционированного доступа, распространения и использования.

1.3 Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», указом Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера, постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», Уставом Университета и иными действующими нормативно-правовыми актами Российской Федерации и локальными нормативными актами Университета.

1.4. Правила обработки и использования персональных данных абитуриентов и обучающихся устанавливаются данным Положением, а также отдельными регламентами и инструкциями Университета.

1.5. Настоящее Положение и изменения к нему утверждаются ректором, вводятся в действие приказом по Университету и доводятся до сведения абитуриентов и обучающихся.

2. ОСНОВНЫЕ ПОНЯТИЯ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В настоящем Положении будут использоваться следующие термины и определения:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), являющемуся абитуриентом или обучающимся Университета;

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. В рамках настоящего Положения оператором является Университет;

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию,

накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

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

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

общедоступные персональные данные – персональные данные, к которым доступ неограниченного круга лиц предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

конфиденциальность персональных данных – обязательное для соблюдения назначенным ответственным лицом, получившим доступ к персональным данным абитуриента и обучающегося, требование не раскрывать третьим лицам и не допускать их распространения без согласия абитуриента и обучающегося, если иное не предусмотрено федеральным законом;

абитуриент – лицо, поступающее в учебное заведение;

обучающиеся – студенты, аспиранты, слушатели и другие категории лиц в соответствии с законодательством об образовании Российской Федерации (ст. 33 Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»).

2.2. В состав персональных данных обучающегося и абитуриента согласно перечню (Приложения № 6,7) входят:

- фамилия, имя, отчество;
- факультет/институт/филиал (кафедра);
- группа;
- сведения об ученых степенях и званиях;
- сведения о результатах вступительных испытаний;
- анкетные и биографические данные;
- сведения об образовании;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- специальность (аспирантов, обучающихся);
- занимаемая должность (аспирантов, обучающихся);
- адрес по месту фактического проживания;

- номер контактного телефона;
- содержание договора на обучение;
- данные из личного дела (приказы);
- перечень изученных, изучаемых дисциплин, в том числе факультативных дисциплин;
- успеваемость, в том числе результаты промежуточной и итоговой аттестации;
- сведения о выплачиваемой стипендии, материальной помощи;
- данные о публикациях и участии в грантах (конкурсах);
- данные о профессии;
- сведения о совершенных правонарушениях;
- сведения о владении иностранными языками;
- данные о наградах и поощрениях (олимпиадах);
- фотографическое изображение (содержащееся в личном деле, студенческом билете, пропуске, зачетной книжке обучающегося);
- банковские реквизиты обучающегося;
- сведения о поступлении (основа обучения, форма обучения, категория набора, год поступления, № зачетной книжки);
- сведения по отпускам (академический);
- социальные льготы;
- место и дата регистрации (вид на жительство, регистрация миграционной карты);
- адрес электронной почты;
- сведения о договорах;
- страховое свидетельство государственного пенсионного страхования;
- сведения о состоянии здоровья;
- иные сведения, с которыми абитуриент и обучающийся считает нужным ознакомить Университет, либо дополнительная информация необходимая Университету.

2.3. Бумажные носители, являющиеся источником персональных данных:

- паспорт или иной документ, удостоверяющий личность;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- приказы по личному составу обучающегося, основания к ним;
- бухгалтерские документы о начислении стипендии обучающегося;
- личные дела абитуриентов и обучающихся;
- зачетные книжки;
- копии указанных выше документов.

2.4. Автоматизированной информационной системой персональных данных абитуриентов и обучающихся в Университете является «ТАНДЕМ. Университет».

3. ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Персональные данные абитуриента и обучающегося следует получать у него самого. Если персональные данные возможно получить только у третьей стороны, то абитуриент и обучающийся должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Университет должен сообщить абитуриенту и обучающемуся о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа абитуриента и обучающегося дать письменное согласие на их получение.

3.2. Университет не имеет права получать и обрабатывать персональные данные абитуриента и обучающегося, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни.

3.3. При поступлении на учебу в Университет абитуриент представляет в приемную комиссию Университета следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ (или копия), удостоверяющий личность, гражданство;
- документ об образовании (или копия);
- фотографии;

- в отдельных случаях с учетом специфики поступления в Университет действующим законодательством Российской Федерации может предусматриваться необходимость предъявления дополнительных документов (например, поступления в вуз иностранных граждан, инвалидов, детей-сирот, военнослужащих и т.д., а также документы о результатах олимпиад, состоянии здоровья и прочее).

3.4. После того, как будет принято решение о зачислении на обучение, а также впоследствии в процессе обучения, к документам, содержащим персональные данные обучающегося, также будут относиться:

- приказ о зачислении в Университет;
- приказы о поощрениях и взысканиях;
- медицинская справка формы № 086 У;
- удостоверение гражданина, подлежащего призыву на военную службу или военный билет;
- приказы, связанные с прохождением учебы.

3.5. Доступ к персональным данным абитуриента и обучающегося имеют:

- ректор и проректоры;
- главный бухгалтер;
- начальник учебно-методического управления;
- начальник финансово-экономического управления;
- начальник управления социальной и внеучебной работы;
- начальник штаба ГОиЧС;
- работники управления бухгалтерского учета и контроля;
- работники режимно-секретного отдела (1-й отдел);
- работники деканатов;
- работники учебно-методического управления;
- члены приемной комиссии;
- работники второго управления;
- программисты ЦНИТ;
- руководители структурных подразделений, деканы, заведующие кафедрами, преподаватели, специалисты по УМР - в отношении персональных данных абитуриентов и обучающихся;
- руководители и работники структурных подразделений в рамках выполнения своих должностных обязанностей;
- работники, осуществляющие архивную обработку документов;
- сам абитуриент и обучающийся, носитель персональных данных и их представители.

4. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных абитуриентов и обучающихся ограничивается достижением конкретных, заранее определенных и законных целей.

4.1.1. Университетом не допускается обработка персональных данных абитуриентов и обучающихся, несовместимая с целями сбора персональных данных.

4.1.2. Университетом не допускается объединение баз данных, содержащих персональные данные абитуриентов и обучающихся, обработка которых осуществляется в целях, несовместимых между собой.

4.2. Обработке подлежат только те персональные данные абитуриентов и обучающихся, которые отвечают целям их обработки.

4.3. Содержание и объем обрабатываемых персональных данных абитуриентов и обучающихся должны соответствовать заявленным целям обработки.

4.4. При обработке персональных данных абитуриентов и обучающихся обеспечивается их точность и достаточность.

4.5. В целях обеспечения прав и свобод человека и гражданина Университет при обработке персональных данных абитуриента и обучающегося обязан соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия абитуриентам и обучающимся в обучении, обеспечения личной безопасности, контроля количества и качества учебной нагрузки.

- при определении объема и содержания, обрабатываемых персональных данных абитуриента и обучающегося Университет должен руководствоваться Конституцией Российской Федерации и иными федеральными законами и подзаконными нормативными актами.

- Работники Университета, имеющие доступ к персональным данным абитуриентов и обучающихся имеют право получать только те персональные данные абитуриентов и обучающихся, которые необходимы для выполнения конкретных трудовых функций.

4.6. Обработка персональных данных абитуриентов и обучающихся осуществляется на основании их письменного согласия на обработку персональных данных (*Приложение № 2*).

4.7. Личное дело содержит персональные данные обучающегося и включает в себя все распоряжения и приказы, касающиеся обучающегося, все заявления обучающегося (о предоставлении материальной помощи, о продлении сессии и др.), медицинские справки. Личное дело пополняется на протяжении всего периода обучения.

4.8. Личное дело абитуриента в обязательном порядке включает в себя заявление о поступлении, документы об образовании для участия в конкурсе и др. документы, предусмотренные законодательством об образовании Российской Федерации.

5. ХРАНЕНИЕ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Хранение персональных данных абитуриента и обучающегося осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в их достижении.

5.2. Доступ к персональным данным абитуриента и обучающегося имеют работники Университета, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей.

5.3. В случае если Университету оказывают услуги юридические и физические лица на основании заключенных договоров, и им необходимо иметь доступ к персональным данным абитуриентов и обучающихся, то соответствующие данные предоставляются только после подписания с ними Соглашения о неразглашении конфиденциальной информации.

5.4. Персональные данные абитуриента (по заявлению на поступление) заносятся в автоматизированную информационную систему «ТАНДЕМ. Университет». После зачисления абитуриента, его персональные данные (в статусе обучающегося) отображаются в информационной системе «ТАНДЕМ. Университет» по отборочным комиссиям структурных подразделений с разграничением прав доступа. Персональные данные не поступивших абитуриентов, хранятся в течение шести месяцев с начала учебного года в соответствии с Порядком приема граждан в образовательные организации высшего образования, затем уничтожаются.

5.5. Личные дела хранятся в бумажном виде в папках и находятся в шкафах, сейфах или в несгораемых шкафах. Персональные данные абитуриентов и обучающихся хранятся также в электронном виде.

5.6. Доступ к электронным базам данных, содержащим персональные данные абитуриентов и обучающихся, обеспечиваются системой паролей. Пароли устанавливаются

работниками Центра новых информационных технологий (ЦНИТ) и сообщаются индивидуально работникам деканата, управления бухгалтерского учета и контроля, учебно-методического управления и другим работникам, имеющим доступ к персональным данным абитуриентов и обучающихся.

5.7. Медицинские сведения об обучающихся хранятся в бумажном виде в личных делах и хранятся согласно п. 5.5.

5.8. Хранение персональных данных обучающихся в структурных подразделениях Университета, работники которых имеют право доступа к персональным данным, осуществляется в порядке, исключающем к ним доступ третьих лиц.

5.9. Защита персональных данных абитуриентов и обучающихся от неправомерного их использования или утраты обеспечивается Университетом.

5.10. Защите подлежат:

- информация о персональных данных абитуриентов и обучающихся;
- документы, содержащие персональные данные абитуриента и обучающегося;
- персональные данные абитуриентов и обучающихся содержащиеся на электронных носителях.

5.11. Перечень допущенных к обработке персональных данных абитуриентов и обучающихся Университета утверждается приказом ректора.

5.12. Работники Университета, имеющие доступ к персональным данным абитуриента и обучающегося, обязаны применять организационно-технические меры по защите персональных данных согласно настоящему Положению, своим должностным инструкциям и прочим нормативным документам Университета, регламентирующим процесс защиты персональных данных.

5.13. Обо всех фактах и попытках нарушения безопасности персональных данных абитуриентов и обучающихся работники, имеющие допуск к обработке персональных данных, обязаны поставить в известность руководителя структурного подразделения.

5.14. При передаче персональных данных третьей стороне должен использоваться безопасный канал передачи. Запрещается передавать персональные данные через сеть международного информационного обмена (отправлять по электронной почте и т.п.) без применения необходимых программных и/или аппаратных средств защиты.

5.15. Университет контролирует соблюдение требований законодательства по защите персональных данных и организывает мероприятия по их реализации. ЦНИТ Университета обеспечивает техническое обслуживание и сопровождение программных средств и ЭВМ с целью защиты персональных данных.

5.16. Работник Университета, имеющий доступ к персональным данным абитуриентов и обучающихся в связи с исполнением трудовых обязанностей:

- обеспечивает хранение информации, содержащей персональные данные абитуриента и обучающегося, исключающее доступ к ним третьих лиц;

- в отсутствие работника на его рабочем месте не должно быть документов, содержащих персональные данные абитуриентов и обучающихся. В процессе работы, документы, содержащие персональные данные, могут находиться на рабочих столах или в специальных папках в течение рабочего дня. По окончании рабочего дня данные документы должны убираться в места постоянного хранения, исключающие к ним доступ третьих лиц. Персональный компьютер, на котором ведется обработка персональных данных, должен быть защищен паролем, а при отсутствии работника на рабочем месте должен блокироваться;

- при уходе в отпуск, нахождение в служебной командировке и иных случаях длительного отсутствия работника на своем рабочем месте, он обязан передать документы и иные носители, содержащие персональные данные абитуриентов и обучающихся лицу, на которое локальным актом Университета (приказом, распоряжением) будет возложено исполнение его трудовых обязанностей.

5.17. При увольнении работника, имеющего доступ к персональным данным абитуриентов и обучающихся, документы и иные носители, содержащие персональные данные, передаются

вновь назначенному на эту должность или другому работнику, имеющему доступ к персональным данным по письменному распоряжению ректора Университета.

5.18. Процедура оформления доступа к персональным данным абитуриентов и обучающихся включает в себя ознакомление работника под роспись с настоящим Положением.

5.19. Абитуриент и обучающийся имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи (за исключением случаев предусмотренных федеральным законом), содержащей его персональные данные. Абитуриент и обучающийся имеет право вносить предложения по внесению изменений в свои данные в случае обнаружения в них неточностей.

6. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Передача персональных данных абитуриента и обучающегося третьей стороне возможна только с письменного согласия абитуриента и обучающегося.

6.1.1. При передаче персональных данных абитуриента и обучающегося Университет должен соблюдать следующие требования:

- не сообщать персональные данные абитуриента и обучающегося третьей стороне без письменного согласия абитуриента и обучающегося;

- не сообщать персональные данные абитуриентов и обучающихся в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные абитуриентов и обучающихся, 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 абитуриента и обучающегося, обязаны соблюдать их конфиденциальность;

- передавать персональные данные абитуриента и обучающегося в порядке, установленном законодательством Российской Федерации;

- передавать персональные данные абитуриента и обучающегося в иные структурные подразделения в случае необходимости исполнения работниками соответствующих структурных подразделений своих трудовых обязанностей.

6.2. Без письменного согласия сведения, содержащие персональные данные, могут быть предоставлены третьим лицам в соответствии с действующим законодательством, если обработка персональных данных необходима в связи с осуществлением правосудия, обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

6.3. Представителю абитуриента и обучающегося персональные данные передаются в порядке, установленном действующим законодательством и настоящим Положением. Информация передается при наличии одного из документов:

- нотариально удостоверенной доверенности представителя обучающегося;

- письменного заявления абитуриента и обучающегося, написанного в присутствии работника управления профориентации и приема, учебно-методического управления, управления аспирантуры или соответствующего деканата Университета (если заявление написано не в присутствии работника вышеуказанного структурного подразделения, то оно должно быть нотариально заверено).

Доверенности и заявления хранятся в личном деле абитуриента и обучающегося.

6.4. Все меры конфиденциальности при сборе, обработке и хранении персональных данных абитуриента и обучающегося распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

6.5. Не допускается отвечать на вопросы, связанные с передачей персональных данных абитуриента и обучающегося по электронной почте, телефону или факсу, кроме общедоступных сведений (Приложение №5).

6.6. Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных несет работник, а также руководитель структурного подразделения, осуществляющего

передачу персональных данных абитуриента и обучающегося третьим лицам.

6.7. Трансграничная передача персональных данных.

6.7.1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

6.7.2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

6.7.3. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- предусмотренных международными договорами Российской Федерации;
- предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;
- исполнения договора, стороной которого является субъект персональных данных;
- защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

7. ОБЯЗАННОСТИ УНИВЕРСИТЕТА

7.1. Университет обязан осуществлять защиту персональных данных абитуриента и обучающегося, применяя все необходимые правовые, организационные и технические меры.

7.2. Университет обязан безвозмездно предоставить абитуриенту и обучающемуся или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему абитуриенту и обучающемуся.

7.3. Университет обязан вносить в персональные данные абитуриента и обучающегося необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему абитуриенту и обучающемуся и обработку которых осуществляет Университет, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Университет обязан уведомить субъекта персональных данных или его законного представителя.

7.4. В случае выявления неправомерной обработки персональных данных Университет в срок, не превышающий трех рабочих дней с даты такого выявления, обязан прекратить неправомерную

обработку персональных данных. В случае если обеспечить правомерность обработки персональных данных невозможно, Университет 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 Университет обязан уведомить субъекта персональных данных или его законного представителя.

7.5. В случае отзыва абитуриентом или обучающимся согласия на обработку своих персональных данных Университет обязан прекратить обработку персональных данных или обеспечить прекращение такой обработки и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Университетом и абитуриентом / обучающимся. Об уничтожении персональных данных и последствиях их уничтожения Университет обязан уведомить абитуриента / обучающегося.

8. ОБЯЗАННОСТИ И ПРАВА АБИТУРИЕНТОВ И ОБУЧАЮЩИХСЯ

8.1. В целях обеспечения достоверности персональных данных абитуриент и обучающийся обязаны:

8.1.1. При поступлении на обучение предоставить Университету полные достоверные данные о себе.

8.1.2. В случае изменения сведений, составляющих персональные данные, незамедлительно предоставить данную информацию в деканат, приемную комиссию или во второе управление Университета.

8.2. Абитуриент и обучающийся имеет право:

8.2.1. на получение сведений об Университете, о месте его нахождения, о наличии у Университета персональных данных, относящихся к самому субъекту персональных данных, а также на ознакомление с такими персональными данными и получения копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;

8.2.2. требовать от Университета уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

8.2.3. на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;

8.2.4. на получение полной информации об обработке своих персональных данных;

8.2.5. на обжалование действий или бездействия Университета в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

8.2.6. на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке).

8.3. Абитуриент и обучающийся несет персональную ответственность за предоставление заведомо неверных данных.

9. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ АБИТУРИЕНТОВ И ОБУЧАЮЩИХСЯ

9.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных абитуриентов и обучающихся, установленных действующим законодательством, Положением о конфиденциальной информации и коммерческой тайне ФГБОУ ВО «ИГУ» и настоящим Положением, несут дисциплинарную, административную, гражданскую или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

Федерации.

9.2. Руководители структурных подразделений, в которых происходит обработка персональных данных, несут персональную ответственность за обеспечение защиты обрабатываемых и хранящихся в их подразделениях персональных данных абитуриентов и обучающихся.

9.3. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается на руководителей структурных подразделений и конкретных должностных лиц Университета, обрабатывающих персональные данные.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

10.1. Настоящее Положение обязательно для всех абитуриентов и обучающихся Университета и лиц, осуществляющих в соответствии со своими должностными обязанностями обработку и использование персональных данных.

III. ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНТРАГЕНТОВ ФГБОУ ВО «ИГУ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящим Положением об обработке и защите персональных данных контрагентов (далее – Положение) устанавливается порядок обработки персональных данных контрагентов федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский государственный университет» (далее – Университет или Оператор) и гарантии конфиденциальности сведений, предоставляемых контрагентами Университету.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информатизации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и иными нормативными актами, действующими на территории Российской Федерации.

1.3. Действие настоящего Положения распространяется на всех работников Университета и доводится до сведения работников под подпись.

1.4. Настоящее Положение вступает в силу со дня его утверждения ректором Университета. Все изменения в настоящее положение вносятся приказом ректора Университета.

1.5. В настоящем Положении используются следующие термины и определения:

- Оператор – Университет. Осуществляет обработку персональных данных, а также определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными контрагентов.

- Контрагент – физическое лицо, официальный представитель – физическое лицо юридического лица и/или индивидуального предпринимателя, вступившее в договорные отношения с Университетом.

- Персональные данные Контрагента – персональные данные, необходимые Оператору в связи с исполнением договорных отношений и касающаяся конкретного Контрагента, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное положение, образование, профессия (должность), номер контактного телефона, адрес электронной почты.

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

- Защита персональных данных Контрагента – деятельность Университета по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер обеспечения конфиденциальности информации.

- Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения и передачи третьим лицам без согласия субъекта персональных данных или наличия иного законного основания.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные Контрагента относятся к категории конфиденциальной информации.

2.2. В целях обеспечения прав и свобод человека и гражданина Оператор и его представители при обработке персональных данных Контрагента соблюдают следующие общие требования:

- обработка персональных данных Контрагента осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством Российской Федерации.
- все персональные данные Контрагента Оператор получает у него самого, за исключением случаев, когда их получение возможно только у третьей стороны способом, не противоречащим законодательству Российской Федерации.
- обработка персональных данных, полученных от третьих лиц, возможна только при уведомлении субъекта персональных данных об этом заранее.

2.3. Оператор не получает и не обрабатывает персональные данные Контрагента о его политических, религиозных и иных убеждениях и частной жизни.

2.4. Персональные данные не используются в целях причинения имущественного и морального вреда Контрагенту, затруднения реализации его прав и свобод.

2.5. При принятии решений, затрагивающих интересы Контрагента, Оператор не основывается на персональных данных Контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

2.6. При идентификации Контрагента Оператор требует предъявление документов, удостоверяющих личность и подтверждающих полномочия представителя.

2.7. При заключении договора, как и в ходе его исполнения, в случае возникновения необходимости, Заказчик может потребовать предоставления Контрагентом иных документов, содержащих информацию о нем, с момента предоставления которых может быть связано предоставление дополнительных гарантий и компенсаций.

2.8. После принятия решения о заключении договора или предоставления документов, подтверждающих полномочия представителя, а также впоследствии, в процессе выполнения договора, персональные данные Контрагента, также будут включены в:

- договоры;
- иные документы, включение в которые персональных данных Контрагента необходимо согласно действующему законодательству Российской Федерации (накладные, акты, отчеты и т.д.).

3. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Все работники, имеющие доступ к персональным данным Контрагентов, подписывают «Соглашение о неразглашении конфиденциальной информации».

3.2. Защита персональных данных Контрагентов от неправомерного их использования или утраты обеспечивается Оператором в порядке, установленном законодательством Российской Федерации, внутренними регламентирующими документами Университета.

3.3. Защите подлежат:

- персональные данные, содержащиеся на электронных и материальных носителях;
- носители, содержащие персональные данные.

3.4. Ответственные лица структурных подразделений Университета, хранящих персональные данные на бумажных и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования.

3.5. Ответственные лица, обрабатывающие персональные данные в информационных системах персональных данных и на машинных носителях информации, обеспечивают защиту в соответствии с требованиями законодательства Российской Федерации, нормативными и методическими документами, касающимися защиты персональных данных.

4. ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Сведения о Контрагентах на бумажных носителях хранятся в помещениях Университета. Для хранения носителей используются шкафы (ящики), расположенные внутри контролируемой зоны Университета.

4.2. Обязанности по хранению документов, в которых содержатся персональные данные Контрагентов, возлагаются на руководителей структурных подразделений, в которых обрабатывается информация.

4.3. Ключи от шкафов /ящиков (при наличии), в которых хранятся носители ПДн, находятся у работника, обрабатывающего данную информацию.

4.4. Персональные данные Контрагентов могут также храниться в электронном виде – на электронных носителях информации, доступ к которым ограничен и регламентируется Университетом.

4.5. Доступ к персональным данным Контрагентов без специального разрешения имеют работники, занимающие в Университете следующие должности:

- ректор;
- проректор;
- главный бухгалтер;
- начальник ФЭУ;
- начальник юридического управления;
- начальник контрактной службы;
- начальник и технические секретари приемной комиссии (работники управления профориентации и приема);
- начальник АХЧ.

4.6. К обработке персональных данных Контрагентов допускаются работники Университета в соответствии с "Перечнем должностей, допущенных к обработке персональных данных" утвержденным ректором Университета.

4.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, по достижении целей обработки или в случае утраты необходимости в их достижении, если иное не предусмотрено законодательством Российской Федерации, вышеуказанные персональные данные уничтожаются.

5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При передаче персональных данных Контрагента Оператор соблюдает следующие требования, и выполняются следующие условия:

- осуществляет обработку персональных данных Контрагента в пределах своей организации в соответствии с настоящим Положением;
- разрешает доступ к персональным данным Контрагентов только специально уполномоченным лицам, при этом указанные лица вправе получать только те персональные данные Контрагента, которые необходимы для выполнения конкретных функций;

- вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством;

- определяет требования к защите обрабатываемых персональных данных и перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, а так же устанавливает обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке;

- в случае если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором;

- передает персональные данные Контрагента его представителям в порядке, установленном законодательством Российской Федерации, и ограничивает эту информацию только теми персональными данными Контрагента, которые необходимы для выполнения указанными представителями их функций.

5.2. В случае если Оператору оказываются услуги, выполняются работы или осуществляется поставка товаров юридическими или физическими лицами на основании заключенных договоров (либо иных оснований), и в силу данных договоров эти лица должны иметь доступ к персональным данным, то необходимые персональные данные предоставляются Оператором при наличии в заключенном договоре условия о неразглашении конфиденциальной информации (в том числе содержащей персональные данные или составляющую коммерческую тайну) либо после подписания с указанными лицами Соглашения о неразглашении информации, содержащей персональные данные (неразглашении конфиденциальной информации).

5.3. Все сведения о передаче персональных данных Контрагентов регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

6. ОБЯЗАННОСТИ КОНТРАГЕНТА И ОПЕРАТОРА

6.1. В целях обеспечения достоверности персональных данных, Контрагент обязан:

- при заключении договора предоставить Оператору полные и достоверные данные о себе;
- в случае изменения сведений, составляющих персональные данные Контрагента, не позднее пяти рабочих дней, предоставить обновленную информацию Оператору.

6.2. Оператор обязан:

- обеспечить защиту персональных данных от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации;

- ознакомить субъекта персональных данных с действующими внутренними правилами обработки персональных данных;

- обеспечить защищенное хранение документов, содержащих персональные данные. При этом персональные данные не должны храниться дольше, чем этого требуют цели, для которых они были получены, или дольше, чем это требуется в интересах лиц, о которых собраны данные, или дольше, чем этого требует законодательство;

- вести учет передачи персональных данных Контрагентов третьим лицам путем ведения соответствующего Журнала учета передачи персональных данных;

- в случае реорганизации или ликвидации Оператора, учет и сохранность документов, порядок передачи их на государственное хранение осуществлять в соответствии с правилами,

предусмотренными учредительными документами и действующим законодательством Российской Федерации;

- вести Журнал учета обращений субъектов персональных данных;
- осуществлять передачу персональных данных субъекта только в соответствии с законодательством Российской Федерации и настоящим Положением;
- по требованию субъекта персональных данных или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных.

7. ПРАВА КОНТРАГЕНТОВ В ЦЕЛЯХ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, Контрагенты имеют право на:

- получение полной информации о составе своих персональных данных и их обработке, в частности, Контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных;
- бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Контрагента на основании письменного запроса, за исключением случаев, если предоставление персональных данных нарушает конституционные права и свободы других лиц;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных. При отказе Оператора исключить или исправить персональные данные Контрагента он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия;
- требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные Контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суде или надзорном органе любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

8. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ПОЛУЧЕНИЕ, ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Лица, виновные в нарушении норм, регулирующих обработку персональных данных, привлекаются к ответственности в соответствии с действующим законодательством Российской Федерации.

IV. ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИХ ЛИЦ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иными нормативными правовыми актами.

Настоящее Положение определяет порядок работы ФГБОУ ВО «ИГУ» (далее - Университет) с персональными данными третьих лиц.

К третьим лицам настоящее положение относит физических лиц, отношения с которыми возникают у Университета при осуществлении предусмотренной Уставом деятельности.

1.2. Настоящее Положение устанавливает порядок обработки персональных данных третьих лиц с использованием и без использования средств автоматизации.

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечению срока хранения, если иное не определено законом.

1.4. Персональные данные третьих лиц не могут быть использованы в целях причинения им имущественного и морального вреда, затруднения реализации их гражданских прав и свобод.

1.5. Сбор, хранение, использование и распространение информации о частной жизни третьих лиц не допускаются.

1.6. Настоящее Положение и изменения к нему утверждаются ректором Университета.

1.7. Настоящее Положение доводится до сведения работников Университета под роспись и является обязательным для исполнения всеми работниками Университета.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Персональные данные третьих лиц (далее - персональные данные) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.2. К персональным данным, обрабатываемым Университетом и подлежащим хранению в порядке, предусмотренном действующим законодательством, относятся следующие сведения:

- Фамилия, имя, отчество;
- Паспортные данные;
 - число, месяц, год рождения;
 - место рождения;
 - серия, номер документа подтверждающего личность, наименование органа, выдавшего его, дата выдачи.
- Контактные данные:
 - адрес (места жительства, регистрации);
 - контактный телефон;
 - адрес электронной почты.

2.3. Персональные данные, перечисленные в п.2.2. настоящего положения являются конфиденциальными. Под конфиденциальностью персональных данных понимается обязательное для соблюдения лицом, получившим доступ к персональным данным третьего лица, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

3. ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. В целях обеспечения прав и свобод человека и гражданина при обработке персональных данных третьих лиц обязательно соблюдаются следующие общие требования:

3.1.1. Обработка персональных данных должна осуществляться на основе принципов законности целей и способов обработки персональных данных и добросовестности; соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных; соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных; достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

3.1.2. Обработка персональных данных может осуществляться Университетом с согласия субъекта персональных данных, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

3.1.3. Обработка персональных данных может осуществляться исключительно в целях осуществления Университетом деятельности, предусмотренной Уставом.

3.1.4. Объем и содержание обрабатываемых персональных данных определяются в соответствии с Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», иными федеральными законами и нормативными правовыми актами.

3.1.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

3.1.6. В случаях достижения цели обработки персональных данных, отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, установленный действующим законодательством.

3.1.7. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена Университетом за счет своих средств в порядке, установленном федеральным законом.

4. ОБЯЗАННОСТИ ТРЕТЬИХ ЛИЦ

Субъект персональных данных обязан:

4.1. Передавать представителю Университета комплекс достоверных документированных персональных данных, перечень которых установлен настоящим Положением.

5. ПРАВА ТРЕТЬИХ ЛИЦ

Физическое лицо, в отношении которого Университет ведет делопроизводство в установленных настоящим Положением целях, имеет право:

5.1. На полную информацию о своих персональных данных и обработке этих данных.

5.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.3. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства. Неправомерный отказ исключить или исправить персональные данные физического лица, а также любое иное нарушение его прав на защиту персональных данных влечет возникновение у физического лица права требовать устранения нарушения его прав и компенсации причиненного таким нарушением морального вреда.

5.4. Принимать предусмотренные законом меры по защите своих прав.

6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных третьих лиц – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или

без использования таких средств с персональными данными третьих лиц, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6.2. Порядок получения персональных данных

6.2.1. Персональные данные следует получать лично у субъекта персональных данных. Получение персональных данных субъекта персональных данных у третьей стороны возможно в случаях, предусмотренных действующим законодательством.

6.2.2. Запрещается получать персональные данные третьего лица о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах, за исключением случаев, предусмотренных действующим законодательством.

6.3. При передаче персональных данных должны соблюдаться следующие требования:

6.3.1. Не сообщать персональные данные третьей стороне, третьим лицам без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных действующим законодательством;

6.3.2. Не использовать персональные данные третьих лиц в коммерческих целях;

6.3.3. Предупредить лиц, получающих персональные данные третьих лиц, 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 третьих лиц, обязаны соблюдать режим конфиденциальности;

6.3.4. Разрешать доступ к персональным данным третьих лиц только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

6.4. Все меры конфиденциальности при обработке персональных данных третьих лиц распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

7. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. Внутренний доступ (доступ внутри Университета).

7.1.1. К обработке персональных данных третьих лиц допускаются работники Университета в соответствии с "Перечнем должностей, допущенных к обработке персональных данных" утвержденным ректором Университета.

7.2. Внешний доступ.

7.2.1. Доступ к персональным данным третьих лиц вне Университета обеспечивается надзорным (контрольным) органам государственной власти и управления, в пределах их компетенции.

8. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Защита персональных данных – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации о конкретном физическом лице.

8.1.1. 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.

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

8.1.3. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, обеспечивающий надежную безопасность информации в процессе деятельности Университета.

8.2. «Внутренняя защита»

8.2.1. Для защиты персональных данных необходимо соблюдение следующих мер:

- ограничение и регламентация состава лиц, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками Университета;
- рациональное размещение рабочих мест работников, исключающее бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- 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 структурных подразделений Университета;
- воспитательная и разъяснительная работа с работниками структурных подразделений Университета по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

8.3. «Внешняя защита»

8.3.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для постороннего лица, пытающегося совершить несанкционированный доступ и овладение информацией.

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

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

8.3.2. Для защиты персональных данных физических лиц необходимо соблюдение следующих мер:

- соблюдение порядка приема, учета и контроля деятельности посетителей;
- организация учета и порядка выдачи удостоверений, пропусков;
- наличие технических средств охраны, сигнализации;
- наличие программных и технических средств защиты информационных систем от несанкционированного доступа;
- обеспечение порядка охраны зданий, помещений.

8.3.3. Все лица, связанные с получением, обработкой и защитой персональных данных третьих лиц обязаны подписать «Соглашение о неразглашении конфиденциальной информации».

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

9.1. Руководитель структурного подразделения, разрешивший доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

9.2. Каждый работник Университета, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

9.3. Лица, виновные в распространении конфиденциальной информации о персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

V. ПОЛОЖЕНИЕ О НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ФГБОУ ВО «ИГУ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и устанавливает единый порядок неавтоматизированной обработки персональных данных в ФГБОУ ВО «ИГУ» (далее – Университет).

1.2. В целях настоящего Положения используются следующие термины и понятия:

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

- обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, уничтожение персональных данных;

- обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, 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.

1.3. Задачи, решаемые в процессе обработки персональных данных:

- документационное обеспечение обработки персональных данных;

- защита документированной информации, содержащей персональные данные.

2. ОСНОВНЫЕ УСЛОВИЯ ПРОВЕДЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных статьей 6 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;

- после направления уведомления об обработке персональных данных в Университет, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;

- после принятия необходимых мер по защите персональных данных.

2.2. В Университете приказом ректора назначается работник, ответственный за организацию обработки и защиту персональных данных, и определяется перечень лиц, допущенных к обработке персональных данных.

2.3. Работники, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением.

2.4. Запрещается обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке.

3. СИСТЕМА ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ДОКУМЕНТАМ

3.1. Система доступа представляет собой совокупность норм и правил, определяющих порядок предоставления работникам прав доступа документам, содержащим конфиденциальную информацию.

3.2. Система доступа должна отвечать следующим требованиям:

- доступ к конфиденциальным документам может предоставляться работникам, письменно оформившим с Университетом соглашение о неразглашении ставших им известными конфиденциальных сведений. Письменное оформление соглашения о неразглашении конфиденциальной информации (соблюдения режима конфиденциальности) является обязательным условием для доступа работников к документам;

- доступ к конфиденциальным документам должен быть обоснованным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного работника;

- система доступа должна давать возможность обеспечивать работников всеми необходимыми им в силу служебных обязанностей документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ;

- доступ к документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению уполномоченного на то должностного лица. При этом соответствующее должностное лицо может давать разрешение на ознакомление с документами только входящими в сферу его деятельности и только установленному кругу лиц;

- доступ к документам осуществляется согласно должностной инструкции.

3.3. Доступ работников Университета к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приеме гражданина на работу или уже в ходе трудовых отношений. При этом соблюдаются следующие условия:

- ознакомление работника под роспись с перечнем конфиденциальной информации;

- ознакомление работника под роспись с установленным в Университете режимом по охране конфиденциальности и с мерами ответственности за его нарушение;

- создание работнику необходимых условий для соблюдения им установленного режима по охране конфиденциальности.

3.4. Доступ работников Университета к персональным данным осуществляется в соответствии с Перечнем допущенных к обработке персональных данных в ФГБОУ ВО «ИГУ».

3.5. Работник принимает следующие обязательства:

- по соблюдению установленного в Университете режима по охране конфиденциальной информации;

- о неразглашении конфиденциальной информации, ставшей ему известной в период выполнения трудовых отношений, после прекращения трудового договора в течение срока, предусмотренного в Соглашении о неразглашении конфиденциальной информации и не использовании этой информации в личных целях;

- о возмещении причиненного ущерба, если работник виновен в разглашении конфиденциальной информации, ставшей ему известной в связи с выполнением им трудовых обязанностей (в том числе после прекращения трудового договора);

- о возврате при прекращении или расторжении трудового договора всех имеющихся у работника материальных носителей конфиденциальной информации.

4. ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

4.1. На бумажных носителях:

4.1.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных и магнитных носителях.

4.1.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

4.1.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных.

4.1.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

4.1.5. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на объекты Университета или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Университета, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на объекты Университета.

4.1.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

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

б) 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.

4.1.7. 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, вымарывание).

4.1.8. Правила, предусмотренные пунктами 4.1.6 и 4.1.7 настоящего Положения, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

4.1.9. 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.

4.2. В электронном виде без использования средств автоматизации:

4.1.1. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на электронных носителях информации.

4.1.2. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

4.1.3. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от иных зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

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

б) 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.

5. ПОДГОТОВКА И УЧЕТ ДОКУМЕНТОВ, СОДЕРЖАЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Бланки типовых форм документов (справки, карточки, талоны, ведомости и т.п.) могут изготавливаться при помощи средств вычислительной техники или на компьютере.

5.2. Персональные данные (переменная часть) в типовые формы документов вносятся при помощи средств вычислительной техники, рукописным способом.

5.3. После внесения переменной части в типовые формы, последние становятся документами и подлежат немедленному учету в журнале изданных документов с присвоением им учетного номера.

6. ПОЛУЧЕНИЕ (ОТПРАВЛЕНИЕ) ДОКУМЕНТОВ И ИХ УЧЕТ

6.1. Все документы, поступающие из иных организаций, подлежат регистрации в журнале учета поступивших документов. На самом документе в правом нижнем углу первого листа документа проставляется отметка о поступлении, которая содержит входящий номер, присвоенный документу, дату поступления.

6.2. Пересылка документов может осуществляться через органы специальной связи или через почтовое отделение связи.

6.3. Об отправленных документах производятся соответствующие отметки в учетных формах.

7. КОПИРОВАНИЕ ДОКУМЕНТОВ

7.1. При действительной служебной необходимости в дополнительных экземплярах документов производится их копирование.

7.2. На некоторых документах может стоять отметка о том, что снятие копий с этого документа не разрешается. Такие документы копированию не подлежат.

7.3. Разрешение на копирование (снятие копий) документов могут давать соответствующие должностные лица (руководители структурных подразделений), наделенные правом распоряжения сведениями.

7.4. Разрешение на изготовление дополнительных экземпляров (копий) учтенного документа оформляется на обороте последнего листа экземпляра, с которого производится копирование. В разрешении указываются номера документов или страниц, с которых необходимо сделать копию, а также количество копий.

8. РЕЖИМ СОХРАННОСТИ ДОКУМЕНТОВ

8.1. Организация хранения документов предполагает, что помещения, где хранятся документы, должны соответствовать требованиям технической безопасности, противопожарной безопасности, а также установленным санитарным нормам.

8.2. Для обеспечения физической сохранности документов, дел, а также для предотвращения разглашения содержащейся в них информации устанавливается специальный режим их хранения и обращения.

8.3. Право входа в такие помещения имеют руководитель организации и работники, имеющие прямое отношение к обработке и хранению документов.

VI. ПОЛОЖЕНИЕ О МЕРАХ ПО ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФГБОУ ВО «ИГУ»

1. ОСНОВНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В Положении используются следующие понятия, определения и сокращения:

ПДн - персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу - субъекту персональных данных.

Обработка ПДн - любое действие с персональными данными, совершаемое с использованием средств автоматизации или без использования таких средств.

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

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Обработка ПДн без использования средств автоматизации - обработка персональных данных, содержащихся в информационной системе персональных данных, либо извлеченных из такой системы, 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.

Актуальные угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Система защиты персональных данных – СЗПДн – правовые, организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Закон «О персональных данных» - Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Приказ ФСТЭК №21 - Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Настоящее Положение о мерах по организации защиты информационных систем персональных данных в ФГБОУ ВО «ИГУ» (далее – Положение) устанавливает состав и содержание правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ФГБОУ ВО «ИГУ» (далее – Университет) на протяжении всего цикла их создания и эксплуатации.

Меры по обеспечению безопасности персональных данных принимаются 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.

Меры по обеспечению безопасности персональных данных реализуются в рамках системы защиты персональных данных, создаваемой Университетом в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных

данных, утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 г. №1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

2.2 Настоящее Положение является внутренним локальным актом Университета.

Настоящее Положение вступает в силу с момента его утверждения ректором Университета и действует бессрочно, до замены его новым Положением.

Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий обработки ПДн.

Изменения к Положению утверждаются ректором Университета.

2.3 Все работники Университета должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

Настоящее Положение является обязательным для исполнения всеми работниками Университета, имеющими доступ к ИСПДн.

2.4 Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм Положения возлагается на назначаемого приказом по Университету уполномоченного сотрудника, ответственного за обеспечение безопасности информационных систем персональных данных.

2.5 Положение разработано с учетом требований принятых в Университете Политики по защите персональных данных в ФГБОУ ВО «ИГУ» и Положения о персональных данных ФГБОУ ВО «ИГУ». Университет учитывает требования настоящего Положения при разработке и утверждении внутренних локальных актов и иных документов Университета, связанных с обработкой ПДн.

3. ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

3.1. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической и видео информации), общесистемное, прикладное, специальное программное обеспечение, а также средства защиты информации.

3.2. Для обеспечения защиты информации, содержащейся в информационной системе, Университетом назначается уполномоченный сотрудник ответственный за обеспечение безопасности информационных систем персональных данных.

3.3. Система защиты персональных данных включает в себя правовые, организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

3.4. Выбор средств защиты информации для системы защиты персональных данных осуществляется Университетом в соответствии с требованиями Приказа ФСТЭК № 21, а также иными нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

3.5. Определение типа угроз безопасности персональных данных, актуальных для информационных систем, производится Университетом с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Закона «О персональных данных».

3.6. Университет обеспечивает классификацию информационных систем в зависимости от того, какие категории персональных данных в ней обрабатываются и какие типы угроз актуальны для ИСПДн Университета. По результатам определяется набор требований, которые необходимо

выполнить для обеспечения того уровня защищенности ПДн, который был определен при классификации ИСПДн Университета.

3.7. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных и контроль за выполнением требований к защите ПДн при обработке их в ИСПДн организуется и проводится Университетом самостоятельно, не реже 1 раза в 3 года в сроки, определяемые Университетом.

4. ОСНОВНЫЕ МЕРЫ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Состав и содержание организационных мер по обеспечению безопасности ПДн.

Необходимый уровень защищенности персональных данных при их обработке в информационных системах Университета обеспечивается принятием следующих основных организационных мер:

- 1) введение режима обеспечения безопасности помещений, в которых размещены ИСПДн Университета, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения и обеспечивается Управлением безопасности ФГБОУ ВО «ИГУ»;
- 2) обеспечение безусловной сохранности носителей персональных данных;
- 3) назначение уполномоченного сотрудника, ответственного за обеспечение безопасности информационных систем персональных данных Университета;
- 4) утверждение перечня персональных данных и иных объектов, подлежащих защите в ИСПДн Университета;
- 5) утверждение перечня лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн Университета, необходим для выполнения ими служебных обязанностей;
- 6) проведение классификации ИСПДн Университета, по результатам определяется набор требований, необходимых для обеспечения необходимого уровня защищенности ПДн;
- 7) обеспечение проведения не реже 1 раза в 3 года проверки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных, и осуществление регулярного контроля за выполнением требований к защите ПДн при обработке их в ИСПДн.

4.2 Мероприятия по реализации организационных мер по обеспечению безопасности ПДн.

С учетом требований, перечисленных в пункте 1 статьи 6 Положения, проводятся следующие мероприятия:

- 1) Приказом ректора назначается уполномоченный сотрудник, ответственный за обеспечение безопасности информационных систем персональных данных Университета. Разрабатывается и вводится в действие должностная инструкция, регламентирующая права и обязанности указанного сотрудника.
- 2) Вводится в действие приказ ректора «О создании Комиссии по персональным данным» (далее по тексту – Комиссия по персональным данным).
- 3) Разрабатывается, утверждается и внедряется система организации доступа в помещения Университета, где осуществляется обработка ПДн, исключающая возможность несанкционированного доступа к техническим средствам обработки ПДн, хищения и нарушения работоспособности ИСПДн, хищения носителей информации ПДн.
- 4) Вводится в действие инструкция о порядке организации внутриобъектового и пропускового режимов в помещениях Университета.

- 5) Определяются состав и категории обрабатываемых в Университете персональных данных (результат оформляется в виде локального нормативного акта с перечнем персональных данных и иных объектов, подлежащих защите в Университете).
- 6) Разрабатывается и вводится в действие инструкция пользователя ИСПДн, регламентирующая права и обязанности работника Университета при работе с ИСПДн.
- 7) Разрабатывается и вводится в действие локальный нормативный акт, регламентирующий разграничение прав доступа к обрабатываемым в ИСПДн персональным данным.
- 8) Подготавливается план обучения работников Университета, осуществляющих обработку ПДн в информационных системах персональных данных, предусматривающий проведение не реже одного раза в год обучения пользования средствами защиты информации, применяемых в информационных системах Университета, правилам работы с ними, правилам обработки ПДн, в соответствии с утвержденными в Университете требованиями.
- 9) Разрабатывается и вводится в действие инструкция о порядке учета, использования, транспортировки, хранения и уничтожения в Университете съемных носителей персональных данных.
- 10) Обеспечивается учет съемных носителей ПДн в каждом структурном подразделении Университета (вводятся в действие журналы учета съемных носителей ПДн).
- 11) Локальными актами регламентирующими обработку и защиту персональных данных работников Университета утверждаются перечни подразделений и работников, допущенных к обработке ПДн в информационных системах Университета.
- 12) Принимается локальный нормативный акт об ответственности работников Университета за разглашение персональных данных и несанкционированный доступ к персональным данным в информационных системах Университета.
- 13) Комиссией по персональным данным проводятся внутренние проверки и классификация ИСПДн Университета. Результаты оформляются в виде письменных отчетов, на основании которых разрабатывается план мероприятий по обеспечению безопасности ПДн в ИСПДн Университета.
- 14) Разрабатывается и утверждается план внутренних проверок состояния защиты ПДн в Университете. Вводится в действие журнал учета мероприятий по контролю соблюдения режима защиты персональных данных в информационных системах Университета.

4.3 Технические меры по обеспечению безопасности ПДн в ИСПДн.

Университет принимает технические меры по обеспечению безопасности информационных систем персональных данных.

План мероприятий по обеспечению защиты персональных данных в Университете включает следующие этапы работы:

- 1) определение на основании Приказа ФСТЭК № 21 базового набора мер по обеспечению безопасности персональных данных в ИСПДн Университета;
- 2) адаптация базового набора мер под ИСПДн Университета с учетом особенностей их функционирования, исключая те меры, которые связаны с информационными технологиями, не используемыми в ИСПДн;
- 3) уточнение списка мер с включением в него не выбранных ранее мер для нейтрализации актуальных угроз;
- 4) внедрение дополнительных мер, обеспечивающих выполнение требований к защите персональных данных, установленных нормативными правовыми актами в

области обеспечения безопасности персональных данных и защиты информации.

В составе мер, входящих в план мероприятий по обеспечению защиты персональных данных в Университете, в том числе, предусматривается:

- 1) внедрение системы парольной аутентификация работников Университета, допущенных к работе с ИСПДн, предусматривающей определение минимальной длины пароля, управление сроком действия и периодической сменой паролей; ограничение числа неудачных попыток входа в систему и использование программных генераторов паролей;
- 2) установление инструктивных и технических правил, обеспечивающих разграничение прав доступа работников к различным ПДн, находящимся в ИСПДн Университета;
- 3) разработка и внедрение регламента обеспечивающего установку и запуск в ИСПДн только разрешенного к использованию в информационной системе программного обеспечения, и исключаяющего возможность использования запрещенного к использованию в информационной системе программного обеспечения;
- 4) разработка инструкции, регламентирующей порядок резервирования и восстановления работоспособности программного обеспечения, баз данных и систем защиты ИСПДн;
- 5) разработка инструкции, регламентирующей модификацию программного обеспечения и технических средств информационной системы персональных данных;
- 6) внедрение технологий, позволяющих осуществлять сбор, запись, хранение, анализ, просмотр и защиту информации о событиях безопасности в ИСПДн Университета;
- 7) использование программного обеспечения по антивирусной защите, обеспечивающего обнаружение в ИСПДн вредоносных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования ПДн, иной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;
- 8) проведение систематических мероприятий по анализу защищенности ИСПДн и тестированию работоспособности системы защиты персональных данных;
- 9) обеспечение защиты ИСПДн, ее средств, систем связи и передачи данных при взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями;
- 10) разработка и ввод в действие электронного журнала учета обращений субъектов персональных данных о выполнении их законных прав, при обработке данных в ИСПДн.

4.4 Предоставление пользователями (посетителями) официального сайта Университета сведений, содержащих персональные данные, осуществляется в соответствии с требованиями, размещенными на сайте Университета в подразделе «Персональные данные» раздела "Сведения об образовательной организации".

5. ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Общее руководство деятельностью Университета по обеспечению безопасности ПДн осуществляет ректор.

5.2 Ректор приказом назначает уполномоченного сотрудника, ответственного за

обеспечение безопасности ИСПДн в Университете.

5.3 Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн в Университете, получает указания непосредственно от ректора.

5.4 Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн в Университете, обязан не реже одного раза в три года проводить проверку состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных, при необходимости вносить предложения по доработке или модернизации системы защиты ПДн.

5.5 Ректор приказом создает в Университете Комиссию по персональным данным, на которую возлагаются следующие обязанности:

- 1) реализация мероприятий, предусмотренных настоящим Положением;
- 2) осуществление внутреннего контроля и аудита соответствия практики обработки персональных данных в Университете тем требованиям и нормам, которые установлены Законом «О персональных данных», а также принятым в этой сфере иным нормативным правовым актам и требованиям к защите персональных данных, и локальным нормативным актам Университета;
- 3) организационное, методическое и научно-техническое руководство работами по созданию либо модернизации системы защиты ПДн.

5.6 Университет на договорной основе имеет право привлечь для разработки и внедрения систем защиты ПДн в ИСПДн Университета специализированные организации, имеющие лицензии ФСТЭК, ФСБ России на соответствующие виды деятельности.

6. ПОРЯДОК МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ПДн

6.1 Для ИСПДн, находящихся в эксплуатации, модернизация или доработка системы защиты ПДн должна проводиться в следующих случаях:

- 1) изменение состава или структуры самой ИСПДн или технических особенностей ее построения (изменение состава или структуры программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);
- 2) изменение состава угроз безопасности ПДн в ИСПДн;
- 3) изменение уровня защищенности, который необходимо обеспечить при защите ПДн.

6.2 Для определения необходимости доработки или модернизации систем защиты ПДн не реже одного раза в три года должна проводиться проверка состава и структуры ИСПДн, состава угроз безопасности ПДн в ИСПДн и эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности персональных данных. Проверка проводится уполномоченным сотрудником, ответственным за обеспечение безопасности ИСПДн. Результаты проверки оформляются Отчетом по проведению внутренней проверки и утверждаются ректором.

7. КОНТРОЛЬ СОБЛЮДЕНИЯ УСЛОВИЙ ИСПОЛЬЗОВАНИЯ СИСТЕМ ЗАЩИТЫ ПДн

7.1 Уполномоченный сотрудник, ответственный за обеспечение безопасности ИСПДн, и Комиссия по персональным данным периодически (не реже одного раза в год) должны проводить проверку соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

7.2 В случае выявления фактов несоблюдения условий хранения носителей ПДн, или использования средств защиты информации, которые могут привести к нарушению заданного уровня безопасности ПДн, либо нарушения заданного уровня безопасности ПДн, должно в обязательном порядке проводиться разбирательство (внутренняя проверка).

7.3 В процессе проведения разбирательства необходимо провести разработку и принятие мер по предотвращению возможных негативных последствий подобных нарушений.

7.4 По окончании проведения разбирательства готовится заключение о лицах, виновных в выявленных нарушениях.

VII. НОРМАТИВНЫЕ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ

При организации и проведении работ по обеспечению безопасности ПДн в Университете, субъекты ПДн должны руководствоваться следующими нормативными и методическими документами:

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 19.12.2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматической обработке персональных данных»;
4. Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
5. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;
6. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
7. Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требования к защите персональных данных при их обработке в информационных системах персональных данных»;
8. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
9. Политика по защите персональных данных в ФГБОУ ВО «ИГУ»;
10. Политика информационной безопасности информационных систем персональных данных ФГБОУ ВО «ИГУ»;
11. Концепция информационной безопасности информационных систем персональных данных ФГБОУ ВО «ИГУ».

ПРИЛОЖЕНИЕ №1
к Положению о персональных данных
ФГБОУ ВО «ИГУ»

СОГЛАСИЕ
работника на обработку персональных данных

Я, _____
(ф.и.о. работника)

зарегистрированный (ая) по адресу: _____

паспорт серия _____ № _____, выдан _____

_____ в соответствии со ст. 9 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» даю согласие на обработку своих персональных данных Федеральному государственному бюджетному образовательному учреждению высшего образования «Иркутский государственный университет» (ФГБОУ ВО «ИГУ») (далее - Оператор), расположенному по адресу: 664003, г. Иркутск, ул. Карла Маркса, д. 1, а именно: совершение действий, предусмотренных п. 3 ст. 3 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных» со всеми данными, которые находятся в распоряжении Оператора.

1. Перечень персональных данных, на обработку которых дается согласие:

фамилия, имя, отчество (в т.ч. предыдущие),
паспортные данные или данные документа, удостоверяющего личность,
дата рождения, место рождения,
гражданство,
отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения,
данные документов о профессиональном образовании, профессиональной переподготовке, повышении
квалификации, стажировке,
данные документов о подтверждении специальных знаний,
данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения
о наградах и званиях,
знание иностранных языков,
семейное положение и данные о составе и членах семьи,
сведения о социальных льготах, пенсионном обеспечении и страховании,
данные документов об инвалидности (при наличии),
данные медицинского заключения (при необходимости),
стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке,
должность, квалификационный уровень,
сведения о заработной плате (доходах), банковских счетах, картах,
адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства,
номер телефона (стационарный домашний, мобильный),
данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (при наличии),
данные страхового свидетельства государственного пенсионного страхования,
данные страхового медицинского полиса обязательного страхования граждан,
личная фотография,
иные сведения, с которыми работник считает нужным ознакомить Оператора, либо дополнительная информация
необходимая Оператору.

2. Цели обработки:

Вышеуказанные персональные данные предоставляю для обработки в целях соблюдения требований трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, продвижении по службе, обеспечения личной безопасности, контроля объема и качества выполняемой работы, обеспечения сохранности имущества, информационного и информационно-аналитического обеспечения образовательной, исследовательской и организационной деятельности Оператора.

3. Перечень действий, на совершение которых дается согласие:

Разрешаю Оператору производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», а именно: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных. Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

4. Согласие на передачу персональных данных третьим лицам:

Разрешаю обмен (прием, передачу, обработку) моих персональными данными между Оператором (организацией-работодателем) и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов.

5. Сроки обработки и хранения персональных данных:

Обработка персональных данных, прекращается после окончания трудового договора работника. В дальнейшем бумажные носители персональных данных находятся на архивном хранении (постоянно или 75 лет), а персональные данные работников на электронных носителях удаляются из информационной системы.

Согласие на обработку данных (полностью или частично) может быть отозвано субъектом персональных данных на основании его письменного заявления.

Права и обязанности в области защиты персональных данных мне разъяснены.

С Положением о об обработке и защите персональных данных Работников ФГБОУ ВО «ИГУ» ознакомлен(а).

Настоящее согласие действует с «___» _____ г.

«___» _____ 201__ г.

(подпись)

**Перечень должностей работников,
имеющих доступ к персональным данным Работников**

1. Доступ к персональным данным работников Университета без специального разрешения имеют работники, занимающие в Университете следующие должности:

- Ректор;
- Проректор;
- Директор института;
- Декан факультета;
- Директор филиала;
- Главный бухгалтер;
- Работники управления бухгалтерского учета и контроля, отвечающие за расчет заработной платы работников Университета, кассовые операции, расчеты с подотчетными лицами;
- Начальник управления кадров;
- Начальник отдела кадров;
- Специалист управления кадров;
- Специалист по кадрам;
- Начальник юридического управления;
- Юрисконсульт;
- Начальник второго управления;
- Главный специалист (по ведению воинского учета и бронированию граждан);
- Начальник финансово-экономического управления;
- Специалисты финансово-экономического управления;
- Работники управления безопасности;
- Начальник отдела охраны труда;
- Ведущий инженер по охране труда и технике безопасности;
- Работники отдела делопроизводства и контроля;
- Заведующий архивом;
- Архивариус;
- Заведующий аспирантурой;
- Ученый секретарь совета;
- Паспортист;
- Работники ЦНИТ, обеспечивающие работоспособность аппаратно-программных средств, предназначенных для автоматизированной обработки персональных данных - к персональным данным, обрабатываемым данными аппаратно-программными средствами;
- Руководители структурных подразделений (факультетов, институтов) - персональным данным работников возглавляемых подразделений;
- Работники приемной комиссии (управления профориентации и приема).

**Акт приема-передачи документов (иных материальных носителей),
содержащих персональные данные Работника**

Во исполнение договора _____ № _____ от «__» _____ 20__ года, заключенного между ФГБОУ ВО «ИГУ», именуемым далее «Заказчик», в лице *Должность ФИО*, действующего на основании _____, и _____ «_____», именуемое в дальнейшем «Исполнитель», в лице *Должность ФИО*, действующего на основании _____,

ЗАКАЗЧИК в лице *Должность ФИО* передает, а ИСПОЛНИТЕЛЬ в лице *Должность ФИО* получает документы (иные материальные носители), содержащие персональные данные Работника Заказчика _____ на срок _____ и в целях:

**Перечень документов (иных материальных носителей),
содержащих персональные данные Работника**

№ п/п		Кол-во
Всего		

Полученные персональные данные Работника могут быть использованы лишь в целях, для которых они сообщены. Незаконное использование предоставленных персональных данных путем их разглашения, уничтожения и другими способами, установленными федеральными законами, может повлечь соответствующую гражданско-правовую, материальную, дисциплинарную, административно-правовую и уголовную ответственность.

Передал

(Ф.И.О., должность работника Университета, осуществляющего передачу персональных данных Работника)

(ПОДПИСЬ)

Принял

(Ф.И.О., должность, представителя организации – приемщика документов (иных материальных носителей),
содержащих персональные данные Работника)

(ПОДПИСЬ)

**Типовая форма
акта об уничтожении носителей, содержащих персональные данные**

Акт № _____
об уничтожении носителей, содержащих персональные данные

Комиссия в составе:

Председатель – _____

Члены комиссии – _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и иной конфиденциальной информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

№ п/п	Дата	Тип носителя	Учетный номер носителя	Категория информации	Примечание

Всего носителей _____
(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем _____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители персональных данных уничтожены путем _____
(разрезания/сжигания/размагничивания/физического уничтожения/ механического уничтожения / иного способа)

Председатель комиссии: _____ / _____ /

Члены комиссии: _____ / _____ /
_____ / _____ /

Перечень категорий персональных данных

ОБЩЕДОСТУПНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Следующие персональные данные являются общедоступными, что означает доступ к этим данным неограниченного круга лиц без соблюдения требования конфиденциальности:

- фамилия, имя, отчество;
- пол;
- факультет (кафедра);
- группа;
- фотографическое изображение;
- сведения о результатах вступительных испытаний.

Эти данные могут публиковаться в общедоступных источниках: стенды, объявления, сайт Университета, публикации, в СМИ и т.п. - с согласия абитуриента и обучающегося.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ ОГРАНИЧЕННОГО ДОСТУПА

Перечень обрабатываемых Университетом персональных данных, на обработку которых необходимо получить согласие абитуриента и обучающегося и на которые распространяется требование конфиденциальности:

- анкетные и биографические;
- сведения об образовании;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- специальность (аспирантов и обучающихся);
- занимаемая должность (аспирантов и обучающихся);
- адрес по месту фактического проживания;
- номер контактного телефона;
- содержание договора на обучение;
- данные из личного дела (приказы);
- перечень изученных, изучаемых дисциплин, в том числе факультативных дисциплин;
- успеваемость, в том числе результаты промежуточной и итоговой аттестации;
- сведения о выплачиваемой стипендии, материальной помощи;
- данные о публикациях и участии в грантах (конкурсах);
- данные о профессии;
- сведения о совершенных правонарушениях;
- сведения о владении иностранными языками;
- данные о наградах и поощрениях (олимпиадах);
- фотографическое изображение (содержащееся в личном деле, студенческом билете, зачетной книжке обучающегося, пропуске);
- банковские реквизиты обучающегося;
- сведения о поступлении (основа обучения, форма обучения, категория набора, год поступления, № зачетной книжки);
- сведения по отпускам (академический);
- социальные льготы;
- место и дата регистрации (вид на жительство, регистрация миграционной карты);
- адрес электронной почты;
- сведения о договорах;
- страховое свидетельство государственного пенсионного страхования;
- сведения о состоянии здоровья;
- иные сведения, с которыми абитуриент и обучающийся считает нужным ознакомить Университет, либо дополнительная информация необходимая Университету в связи с трудовыми отношениями.

СОГЛАСИЕ
обучающегося на обработку персональных данных

Я, _____
(Ф.И.О.)

зарегистрированный(ая) по адресу

паспорт серия _____ № _____ выдан _____, _____
(дата) (кем выдан)

именуемый в дальнейшем Субъект, во исполнение требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» даю добровольное согласие Федеральному государственному бюджетному образовательному учреждению высшего образования «Иркутский государственный университет» (ФГБОУ ВО «ИГУ») (далее - Университет), зарегистрированному по адресу: 664003, г. Иркутск, ул. Карла Маркса, д. 1, на обработку своих персональных данных на следующих условиях:

I. Субъект дает согласие на обработку Университетом своих персональных данных, то есть совершение, в том числе, следующих действий: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, при этом общее описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных».

II. Университет обязуется использовать данные Субъекта только с целью:

- защиты конституционных прав и законных интересов;
- обеспечения права на образование;
- создания благоприятных условий системы образования;
- удовлетворения потребностей личности в интеллектуальном, культурном, в нравственном развитии посредством получения высшего образования, а также дополнительного образования;
- функционирования информационных систем Университета;
- взаимодействия с федеральными органами (министерство образования и науки Российской Федерации, правоохранительные органы, налоговые органы, надзорные органы и др.);
- предоставления персональных данных обучающихся в банки для осуществления расчетов по операциям с использованием банковских карт (далее - карточные счета), выпуска и перевыпуска банковских карт.

III. Перечень персональных данных обучающегося, обрабатываемых Университетом как с использованием автоматизированных средств обработки персональных данных работника, так и без использования средств автоматизации:

- фамилия, имя, отчество;
- пол;
- факультет/институт (кафедра);
- группа;
- сведения об ученых степенях и званиях;
- сведения о результатах вступительных испытаний;
- анкетные и биографические данные;
- сведения об образовании;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- специальность (аспирантов, обучающихся);
- занимаемая должность (аспирантов, обучающихся);
- адрес по месту фактического проживания;
- номер контактного телефона;
- содержание договора на обучение;
- данные из личного дела (приказы);
- перечень изученных, изучаемых дисциплин, в том числе факультативных дисциплин;
- успеваемость, в том числе результаты промежуточной и итоговой аттестации;

- сведения о выплачиваемой стипендии, материальной помощи;
- данные о публикациях и участии в грантах (конкурсах);
- данные о профессии;
- сведения о совершенных правонарушениях;
- сведения о владении иностранными языками;
- данные о наградах и поощрениях (олимпиадах);
- фотографическое изображение для обеспечения однократного и/или многократного прохода на охраняемую территорию Университета (пропуск/допуск);
- цифровая фотография (для оформления электронного читательского формуляра);
- фотографическое изображение (содержащееся в личном деле, студенческом билете, зачетной книжке обучающегося);
- банковские реквизиты обучающегося;
- сведения о поступлении (основа обучения, форма обучения, категория набора, год поступления, № зачетной книжки);
- сведения по отпускам (академический);
- социальные льготы;
- место и дата регистрации (вид на жительство, регистрация миграционной карты);
- адрес электронной почты;
- сведения о договорах;
- сведения о страховой компании;
- страховое свидетельство государственного пенсионного страхования;
- сведения о состоянии здоровья;
- иные сведения, с которыми обучающийся считает нужным ознакомить Университет, либо дополнительная информация необходимая Университету.

IV. Субъект дает согласие на включение в общедоступные источники персональных данных (в соответствии с п. 1 ст. 8 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных») следующих сведений:

- фамилия, имя, отчество;
- пол;
- факультет (кафедра);
- группа;
- сведения об ученых степенях и званиях;
- сведения о результатах вступительных испытаний;
- фотографическое изображение.

Эти данные могут публиковаться в общедоступных источниках: стенды, объявления, сайт Университета, публикации, в СМИ и т.п.

V. Субъект дает согласие на передачу персональных данных в следующие организации:

- Банки, с которыми имеются договорные отношения, в целях перечисления стипендии или иных выплат на его счет и обновления информации о нем, выпуска и перевыпуска банковских карт. Персональные данные передаются банку в течение всего периода обучения субъекта в Университете;
- организации, в том числе государственные и муниципальные органы, имеющие необходимость осуществлять обработку персональных данных, указанных в настоящем Положении;
- иные организации, связанные с Университетом договорными обязательствами.

VI. Субъект дает согласие на трансграничную передачу персональных данных в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

VII. Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии со ст. 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

VIII. Обработка персональных данных прекращается при достижении целей обработки.

IX. Субъект имеет право отозвать согласие на обработку персональных данных путем направления соответствующего заявления в адрес ФГБОУ ВО «ИГУ».

X. Субъект несет ответственность за достоверность представленных сведений в соответствии с пунктом 8.1 Положения о персональных данных абитуриентов и обучающихся ФГБОУ ВО «ИГУ».

XI. Настоящее согласие действует на период обучения субъекта, а также по истечению срока обучения в архивных целях на срок, предусмотренный законодательством Российской Федерации.

С Положением о персональных данных абитуриентов и обучающихся ФГБОУ ВО «ИГУ» ознакомлен(а).

« ___ » _____ 201__ г.

_____ (подпись)

СОГЛАСИЕ
абитуриента на обработку персональных данных

Я, _____
(Ф.И.О.)

зарегистрированный(ая) по адресу

паспорт серия _____ № _____ выдан _____,
(дата) (кем выдан)

именуемый в дальнейшем Субъект, во исполнение требований Федерального закона от 27.07.2006 г. 152-ФЗ «О персональных данных» даю добровольное согласие Федеральному государственному бюджетному образовательному учреждению высшего образования «Иркутский государственный университет» (ФГБОУ ВО «ИГУ») (далее - Университет), зарегистрированному по адресу: 664003, г. Иркутск, ул. Карла Маркса, д. 1, на обработку своих персональных данных на следующих условиях:

I. Субъект дает согласие на обработку Университетом своих персональных данных, то есть совершение, в том числе, следующих действий: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, при этом общее описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных».

II. Университет обязуется использовать данные Субъекта только с целью:

- защиты конституционных прав и законных интересов;
- обеспечения права на образование;
- создания благоприятных условий системы образования;
- удовлетворения потребностей личности в интеллектуальном, культурном, в нравственном развитии посредством получения высшего образования, а также дополнительного образования;
- функционирования информационных систем Университета;
- взаимодействия с федеральными органами (министерство образования и науки Российской Федерации, правоохранительные органы, налоговые органы, надзорные органы и др.).

III. Перечень персональных данных абитуриента, обрабатываемых Университетом как с использованием автоматизированных средств обработки персональных данных работника, так и без использования средств автоматизации:

- фамилия, имя, отчество;
- пол;
- факультет/институт (кафедра);
- группа;
- сведения об ученых степенях и званиях;
- сведения о результатах вступительных испытаний;
- анкетные и биографические;
- сведения об образовании;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- специальность;
- занимаемая должность;
- адрес по месту фактического проживания;
- номер контактного телефона;
- содержание договора на обучение;
- данные из личного дела (приказы);
- перечень изученных, изучаемых дисциплин, в том числе факультативных дисциплин;
- успеваемость, в том числе результаты промежуточной и итоговой аттестации;
- сведения о выплачиваемой стипендии, материальной помощи;
- данные о публикациях и участии в грантах (конкурсах);
- данные о профессии;
- сведения о совершенных правонарушениях;

- сведения о владении иностранными языками;
- данные о наградах и поощрениях (олимпиадах);
- фотографическое изображение;
- сведения о поступлении (основа обучения, форма обучения, категория набора, год поступления, № зачетной книжки);
- социальные льготы;
- место и дата регистрации (вид на жительство, регистрация миграционной карты);
- адрес электронной почты;
- сведения о договорах;
- сведения о страховой компании;
- страховое свидетельство государственного пенсионного страхования;
- сведения о состоянии здоровья;
- иные сведения, с которыми абитуриент считает нужным ознакомить Университет, либо дополнительная информация необходимая Университету.

IV. Субъект дает согласие на включение в общедоступные источники персональных данных (в соответствии с п. 1 ст. 8 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных») следующих сведений:

- фамилия, имя, отчество;
- пол;
- факультет (кафедра);
- группа;
- сведения об ученых степенях и званиях;
- сведения о результатах вступительных испытаний;
- фотографическое изображение.

Эти данные могут публиковаться в общедоступных источниках: стенды, объявления, сайт Университета, публикации, в СМИ и т.п.

V. Субъект дает согласие на передачу персональных данных в следующие организации:

- организации, в том числе государственные и муниципальные органы, имеющие необходимость осуществлять обработку персональных данных, указанных в настоящем Положении;
- иные организации, связанные с Университетом договорными обязательствами.

VI. Субъект дает согласие на трансграничную передачу персональных данных в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

VII. Субъект по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии со ст. 14 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

VIII. Обработка персональных данных прекращается при достижении целей обработки.

IX. Субъект имеет право отозвать согласие на обработку персональных данных путем направления соответствующего заявления в адрес ФГБОУ ВО «ИГУ».

X. Субъект несет ответственность за достоверность представленных сведений в соответствии с пунктом 8.1 Положения о персональных данных абитуриентов и обучающихся ФГБОУ ВО «ИГУ».

XI. Настоящее согласие действует на период обучения субъекта, а также по истечению срока обучения в архивных целях на срок, предусмотренный законодательством Российской Федерации.

С Положением о персональных данных абитуриентов и обучающихся ФГБОУ ВО «ИГУ» ознакомлен(а).

« ___ » _____ 201__ г.

(подпись)

СОГЛАСИЕ

законного представителя несовершеннолетнего субъекта персональных данных

г. Иркутск

«__» _____ 20__ г.

Я, _____,

(ФИО родителя или иного законного представителя несовершеннолетнего лица)

паспорт: серия _____ № _____, выдан _____,

(когда и кем выдан)

(в случае опекуна указать реквизиты документа, на основании которого осуществляется опека или попечительство)

являясь законным представителем несовершеннолетнего ребенка _____,

(ФИО ребенка)

приходящегося мне _____,

(сын, дочь и т.д.)

зарегистрированного по адресу: _____,

даю согласие Федеральному государственному бюджетному образовательному учреждению высшего образования «Иркутский государственный университет» (далее – Университет) на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными вышеуказанного несовершеннолетнего ребенка, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ, в том числе раскрытие неопределенному кругу лиц), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных: фамилия, имя и отчество (прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения); дата и место рождения; сведения о гражданстве (в том числе предыдущее гражданство, иные гражданства); сведения об образовании; информация о владении иностранными языками, уровень владения; спортивное звание, спортивный разряд; адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания; номер контактного телефона или сведения о других способах связи; вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи; отношение к воинской обязанности, сведения по воинскому учету; семейное положение, состав семьи; сведения о трудовой деятельности; государственные награды, иные награды и знаки отличия (кем награжден и когда); информация о наличии либо отсутствии судимости; сведения о пребывании за границей (когда, где, с какой целью); личная фотография.

Вышеуказанные персональные данные предоставляю для обработки в целях информационного обеспечения деятельности, информационно-аналитического обеспечения учебного процесса, исследовательской и организационной деятельности Университета.

Я ознакомлен(а), что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия на период обучения, а также по истечению срока обучения в архивных целях на срок, предусмотренный законодательством Российской Федерации;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных Университет вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;

4) персональные данные хранятся в Университете в течение установленного законодательством Российской Федерации срока хранения документов;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных на Университет полномочий.

Я подтверждаю, что давая такое согласие, я действую по собственной воле и в интересах своего ребенка.

С Положением о персональных данных абитуриентов и обучающихся ФГБОУ ВО «ИГУ» ознакомлен(а).

«__» _____ 201__ г.

_____ (подпись)

_____ (расшифровка подписи)

ОТЗЫВ СОГЛАСИЯ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество полностью)

в соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ "О персональных данных" отзываю у ФГБОУ ВО «ИГУ» согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в связи с

(указать причину)

в срок, не превышающий тридцати дней с момента поступления настоящего отзыва.

«__» _____ 201__ г.

(подпись)

(расшифровка подписи)

ПРИЛОЖЕНИЕ №12
к Положению о персональных данных
ФГБОУ ВО «ИГУ»

Согласие на обработку персональных данных

г. Иркутск

«___» _____ 20__ г.

Я, _____
(фамилия, имя, отчество)

зарегистрированный(ная) по адресу: _____

паспорт: серия _____ № _____ выдан _____
(дата)

(кем выдан)

в соответствии с требованиями ст. 9 Федерального закона от 27.07.06 г. №152-ФЗ «О персональных данных», подтверждаю свое согласие Федеральному государственному бюджетному образовательному учреждению высшего образования «Иркутский государственный университет» (г. Иркутск, ул. Карла Маркса,1) (далее - Оператор) на обработку моих персональных данных, включающих:

- фамилия;
- имя;
- отчество;
- данные документа, удостоверяющего личность;
- пол;
- дата рождения;
- адрес регистрации;
- адрес места жительства;
- контактный телефон;
- электронный адрес почты;
- личная фотография;
- иные сведения.

Предоставляю Оператору осуществлять любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ, в том числе раскрытие неопределенному кругу лиц), обезличивание, блокирование, удаление, уничтожение) любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ, в том числе раскрытие неопределенному кругу лиц), обезличивание, блокирование, удаление, уничтожение).

Я ознакомлен(а), что:

- 1) согласие на обработку персональных данных действует с даты подписания настоящего согласия до достижения цели обработки персональных данных;
- 2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;
- 3) в случае отзыва согласия на обработку персональных данных ФГБОУ ВО «ИГУ» вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- 4) персональные данные хранятся в ФГБОУ ВО «ИГУ» в течение установленного законодательством Российской Федерации срока хранения документов;
- 5) предоставляемые персональные данные будут обрабатываться только в целях соблюдения требований действующего законодательства, информационного и информационно-аналитического обеспечения образовательной, исследовательской, административно-хозяйственной деятельности ФГБОУ ВО «ИГУ».

С Положением о персональных данных третьих лиц ФГБОУ ВО «ИГУ» ознакомлен(а).

«___» _____ 201__ г.

_____ (подпись)

_____ (расшифровка подписи)

СОГЛАШЕНИЕ № _____
о неразглашении конфиденциальной информации.

г. Иркутск

« ____ » _____ 20__ г.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский государственный университет», именуемое в дальнейшем «ФГБОУ ВО «ИГУ» или «Университет», в лице ректора Аргучинцева Александра Валерьевича, действующего на основании Устава, с одной стороны, и

_____,
(ФИО)
зарегистрированный по адресу: г. Иркутск, ул. _____, д. ____, кв. ____,
паспорт РФ: серия _____ № _____, выдан « ____ » _____ 20__ г.

_____, именуемый в
дальнейшем «Работник», с другой стороны, совместно именуемые в дальнейшем «Стороны», заключили
настоящее соглашение о нижеследующем.

1. Работник, в связи с исполнением своих должностных обязанностей, получает доступ к персональным данным сотрудников и обучающихся Университета, иных лиц, участвующих в мероприятиях, организованных Университетом, а также к сведениям, содержащим иную конфиденциальную информацию, доступ к которым ограничен Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и иными правовыми актами, и **обязуется не разглашать ставшие ему известными персональные данные сотрудников и обучающихся Университета, иных лиц, участвующих в мероприятиях, организованных Университетом, иные сведения, содержащие конфиденциальную информацию**, за исключением случаев предусмотренных законодательством Российской Федерации.

2. Под конфиденциальной информацией в настоящем соглашении понимается речевая, аудиовизуальная, документированная информация с ограниченным доступом и иная информация, содержащая охраняемую в соответствии с действующим законодательством тайну Университета, а также персональные данные сотрудников и обучающихся Университета, иных лиц, участвующих в мероприятиях, организованных Университетом. Конфиденциальная информация, содержащаяся в локальной сети Университета, также имеет ограниченный доступ.

К конфиденциальной информации по настоящему соглашению в частности, но не ограничиваясь, относится любая или вся, настоящая или будущая, техническая, финансовая, деловая информация, статистика, данные, схемы, планы, спецификации, документы, идеи, концепции, продукты, процессы, технологии, цены, пароли доступа к информационным системам и другая информация, которая отнесена к конфиденциальной действующим законодательством Российской Федерации и локальными правовыми актами Университета и была передана Работнику для выполнения последним своих трудовых обязанностей.

3. Не могут являться конфиденциальной информацией сведения:

- которые до момента заключения настоящего соглашения были публично обнародованы;
- которые стали общедоступны во время действия настоящего соглашения, но без виновного участия Работника.

4. Вся конфиденциальная информация, полученная Работником в материальной (схемы, рисунки, письма, фотографии и пр.) и нематериальной формах, является собственностью Университета и используется только на условиях настоящего соглашения.

5. Работник обязуется:

5.1. Знать требования Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Положения о персональных данных ФГБОУ ВО «ИГУ», Положения о конфиденциальной информации и коммерческой тайне ФГБОУ ВО «ИГУ».

5.2. Не разглашать и не передавать третьим лицам сведения, являющиеся конфиденциальной информацией, ставшие ему известными в связи с исполнением трудовых обязанностей, а также защищать вышеуказанные сведения от посягательств и попыток ее обнародовать третьими лицами.

5.3. Использовать сведения, полученные при исполнении своих трудовых обязанностей, лишь в интересах Университета.

5.4. В случае увольнения из Университета вернуть все сведения, полученные на материальных носителях, а также их копии, в течение одного дня с момента получения соответствующего требования о возврате.

5.5. Не использовать конфиденциальную информацию после увольнения из Университета.

6. В случае разглашения Работником сведений, являющихся конфиденциальной информацией, трудовой договор с Работником подлежит расторжению в соответствии с подпунктом «в» пункта 6 статьи 81 Трудового кодекса Российской Федерации.

7. В случае разглашения сведений, являющихся конфиденциальной информацией, Работник обязан в полном объеме возместить понесенные в результате такого разглашения Университетом убытки.

8. В случае разглашения конфиденциальной информации Работник может быть привлечен к дисциплинарной, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

9. Настоящее Соглашение действует бессрочно. Прекращение отношений по трудовому договору не является основанием для прекращения обязательств Сторон по настоящему соглашению.

10. Настоящее Соглашение составлено на двух страницах, на одном листе, в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному для каждой Стороны.

Ректор ФГБОУ ВПО «ИГУ»

Работник

_____ А. В. Аргучинцев

_____ / _____

М.П.

СПИСОК ПРИЛОЖЕНИЙ К ПОЛОЖЕНИЮ

Приложение №1. Согласие работника на обработку персональных данных;

Приложение №2. Перечень должностей работников, имеющих доступ к персональным данным Работников;

Приложение №3. Акт приема-передачи документов (иных материальных носителей), содержащих персональные данные Работника;

Приложение №4. Типовая форма акта об уничтожении носителей, содержащих персональные данные;

Приложение №5. Перечень категорий персональных данных;

Приложение №6. Согласие обучающегося на обработку персональных данных;

Приложение №7. Согласие абитуриента на обработку персональных данных;

Приложение №8. Согласие законного представителя несовершеннолетнего субъекта персональных данных;

Приложение №9. Отзыв согласия на обработку персональных данных;

Приложение №10. Журнал учета передачи персональных данных;

Приложение №11. Журнал учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных;

Приложение №12. Согласие на обработку персональных данных;

Приложение №13. Журнал учета съемных носителей конфиденциальной информации (персональных данных);

Приложение №14. Журнал изданных документов;

Приложение №15. Соглашение о неразглашении конфиденциальной информации.