ПОЛИТИКА
Университета в отношении обработки персональных данных
№ 47/07 от 29.08.2012

Утверждено на заседании ученого совета университета (протокол от 29.08.2012 № 1)

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика по защите персональных данных (далее - Политика) в федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Поволжский государственный университет сервиса» (далее – Университет) разработана в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ (с последующими изменениями) и Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

1.2. Цель разработки Политики — определение особенностей обработки и обеспечения безопасности персональных данных, а также минимизация ущерба, который может возникнуть вследствие воздействия угроз информационной безопасности, приводящих к нарушению требуемых свойств безопасности персональных данных.

1.3. Организация хранения, учета и использования персональных данных осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.4. Работники Университета должны быть ознакомлены со внутренней организационно-распорядительной документацией, устанавливающей правила обработки персональных данных, в соответствии с порядком, изложенным в этих внутренних нормативных документах.

1.5. Требования настоящей Политики при необходимости могут детализироваться иными внутренними нормативными документами Университета.

1.6. Все работники Университета, которые участвуют в обработке персональных данных, должны быть ознакомлены с настоящей Политикой под роспись.

## 2. УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

| | |
|---|---|
| **АРМ** | Автоматизированное рабочее место |
| **ИБ** | Информационная безопасность |
| **ИС** | Информационная система |
| **ИСПДн** | Информационная система персональных данных |
| **ЛВС** | Локальная вычислительная сеть |
| **ПДн** | Персональные данные |
| **СЗПДн** | Система защиты персональных данных |

## 3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения;

**Безопасность информации [данных]** - состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

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

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

**Конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

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

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

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

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

**Средства вычислительной техники** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Угрозы безопасности персональных данных** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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

**Уполномоченное оператором лицо** - лицо, которому на основании договора оператор поручает обработку персональных данных.

**Целостность информации** - обеспечение достоверности и полноты информации и методов ее обработки.

## 4. ОБЩИЕ ПОЛОЖЕНИЯ ПО ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

4.1. Основными принципами обработки ПДн являются:

– Обработка персональных данных должна осуществляться на законной и справедливой основе.

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

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

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

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

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

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

4.2. В Университете используется смешанная обработка ПДн. Под смешанной обработкой понимается автоматизированная и неавтоматизированная обработка ПДн. При этом полученная в ходе обработки ПДн информация может:

- передаваться получателю по ЛВС университета;
- передаваться получателю с использованием сети общего пользования Интернет;
- не передаваться.

4.3. В соответствии с Законом № 152-ФЗ в Университет обрабатывает следующие категории ПДн:

- Специальные категории персональных данных: сведения о состоянии здоровья, о наличии/отсутствии судимости.
- ПДн, отнесенные в соответствии с Законом № 152-ФЗ к общедоступным или обезличенным ПДн.

4.5. В случае достижения цели обработки ПДн, если иное не предусмотрено законодательством Российской Федерации. Университет прекращает обработку и производит их уничтожение, или обеспечивает прекращение обработки и уничтожение ПДн, которые обрабатывались третьими лицами на основании договора с Университетом, в порядке, установленном законодательством Российской Федерации о защите персональных данных. Уничтожение ПДн и материальных носителей ПДн в Университете осуществляется в

соответствии с положением «Об организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных университета».

## 5. ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕДУРАМ ОБРАБОТКИ ПДН

5.1. Обработка ПДн в Университете должна осуществляться в соответствии с требованиями статьи 6 Федерального закона № 152-ФЗ.

5.2. В Университете запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн, или иным образом затрагивающих его права и законные интересы, кроме случаев и условий, предусмотренных законодательством Российской Федерации.

5.3. При необходимости Университет осуществляет трансграничную передачу ПДн в соответствии с законодательством Российской Федерации, а также на основе соответствующих соглашений с международными и иностранными организациями, закрепляющих адекватную защиту прав субъектов ПДн, в том числе в части обеспечения конфиденциальности ПДн.

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

5.5. В Университете ведется учет работников, осуществляющих обработку ПДн в ИСПДн. Учет ведет отдел по работе с персоналом совместно с Владельцами ИСПДн и администраторами безопасности ИСПДн в виде электронного перечня и/или списка на основании ОРД и согласованных и исполненных в установленном порядке заявок на доступ в ИСПДн. Учет ведется на основе списков доступа работников и/или установленных ролей в соответствии с занимаемой должностью. Списки сотрудников, допущенных до автоматизированной обработке персональных данных (за исключением общедоступных и обезличенных ПДн) утверждаются приказом Ректора Университета.

5.6. Порядок допуска и доступа к работе в ИСПДн устанавливается согласно «Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных». Доступ к ПДн и обработку таких данных работники Университета должны осуществлять только для выполнения должностных обязанностей.

5.7. Работники Университета, осуществляющие обработку ПДн в ИСПДн, должны быть проинформированы о факте обработки ими ПДн и категориях обрабатываемых ПДн при предоставлении доступа к ИСПДн, а также должны быть ознакомлены пол личную подпись со всей организационно-распорядительной документацией регламентирующей обработку ПДн.

5.8. Все работники университета, осуществляющие обработку ПДн (за исключением общедоступных и обезличенных) подписывают соглашение о неразглашении ПДн.

## 6. СВЕДЕНИЯ О РЕАЛИЗУЕМЫХ В УНИВЕРСИТЕТЕ ТРЕБОВАНИЯХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

6.1. Университет при обработке персональных данных обеспечивает принятие необходимых правовых, организационных и технических мер для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.2. В целях защиты персональных данных Университет реализует требования к защите персональных данных при их обработке в информационных системах персональных данных, установленные Правительством РФ.

6.3. Сведения о предпринимаемых Университетом мерах для защиты персональных данных являются информацией ограниченного доступа.

## 7. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ.

7.1. Университет при обработке ПДн обеспечивает необходимые условия для беспрепятственной реализации субъектом ПДн своих прав.

7.2. Субъект ПДн имеет право на доступ к своим персональным данным. Субъект ПДн имеет право на получение сведений, указанных в части 7 статьи 14 Федерального закона «О персональных данных». Право субъекта ПДн на доступ к своим персональным данным ограничивается в случаях, предусмотренных Федеральным законом «О персональных данных».

7.3. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

## 8. ОБЯЗАННОСТИ РАБОТНИКОВ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПДН

8.1. Работники, допущенные к обработке ПДн, обязаны:

- знать и неукоснительно выполнять требования настоящей Политики;
- обрабатывать ПДн только в рамках выполнения своих должностных обязанностей;
- не разглашать ПДн, полученные в результате выполнения своих должностных обязанностей, а также ставшие им известными по роду своей деятельности;
- пресекать действия других лиц, которые могут привести к разглашению (уничтожению, искажению) ПДн;
- выявлять факты разглашения (уничтожения, искажения) ПДн и информировать об этом администратора ИБ и/или ответственному за обеспечение безопасности персональных данных.

8.2. Обязанности работников, допущенных к обработке ПДн, регламентируются организационно-распорядительной документацией Университета, устанавливающей правила обращения с персональными данными.

## 9. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ НАСТОЯЩЕЙ ПОЛИТИКИ

9.1. Контроль за обеспечением безопасности ПДн и соблюдением требований настоящей Политики осуществляет ответственный за обеспечение безопасности персональных данных.

9.2. Контроль осуществляется путем проведения мониторинга ИБ и менеджмента инцидентов ИБ, по результатам оценки состояния ИБ, а также в рамках иных контрольных

мероприятий.