



**НОВОТРОИЦКИЙ
МУНИЦИПАЛЬ
БОЛЬГЕСИ**

**НОВОТРОИЦКИЙ
МУНИЦИПАЛЬНЫЙ
ОКРУГ**

**НОВОТРОИЦКИЙ
МУНИЦИПАЛЬНИЙ
ОКРУГ**

ул. Соборная, 73, п.г.т. Новотроицкое, Новотроицкий муниципальный округ, Херсонская область, 275300
email: Novotroitsk_admin@khogov.ru

**ПОСТАНОВЛЕНИЕ
ГЛАВЫ НОВОТРОИЦКОГО МУНИЦИПАЛЬНОГО
ОКРУГА ХЕРСОНСКОЙ ОБЛАСТИ**

24.09.2025 № 800

пгт. Новотроицкое

Об утверждении Политики
информационной безопасности в
Администрации Новотроицкого
муниципального округа Херсонской
области, Политики обработки
персональных данных в
Администрации Новотроицкого
муниципального округа Херсонской
области, Политики обработки
персональных данных на
официальных сайтах Администрации
Новотроицкого муниципального
округа

В целях обеспечения соблюдения прав и свобод граждан при обработке их персональных данных, открытости и прозрачности деятельности Администрации Новотроицкого муниципального округа Херсонской области в информационно-телекоммуникационной сети Интернет, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», иными нормативно-правовыми актами Российской Федерации, Уставом муниципального образования Новотроицкого муниципального округа Херсонской области, принятым решением Совета депутатов Новотроицкого муниципального округа Херсонской области от 26.10.2023 № 24, Положением об Администрации Новотроицкого муниципального округа Херсонской области, утверждённым решением Совета депутатов Новотроицкого муниципального округа Херсонской области от 02.11.2023 № 27,

ПОСТАНОВЛЯЮ:

1. Утвердить прилагаемую Политику информационной безопасности в Администрации Новотроицкого муниципального округа Херсонской области (Приложение № 1).

2. Утвердить прилагаемую Политику обработки персональных данных в Администрации Новотроицкого муниципального округа Херсонской области (Приложение № 2).

3. Утвердить прилагаемую Политику обработки персональных данных на официальных сайтах Администрации Новотроицкого муниципального округа (Приложение № 3).

4. Разместить Политику информационной безопасности в Администрации Новотроицкого муниципального округа Херсонской области, Политику обработки персональных данных в Администрации Новотроицкого муниципального округа Херсонской области, Политику обработки персональных данных на официальных сайтах Администрации Новотроицкого муниципального округа на официальных сайтах Администрации Новотроицкого муниципального округа Херсонской области в информационно-телекоммуникационной сети Интернет по адресам:

<https://novotroick-r74.gosweb.gosuslugi.ru>

<https://novotroitskoe.gosuslugi.ru>

3. Контроль за выполнением настоящего постановления оставляю за собой.

4. Настоящее постановление вступает в силу после его официального опубликования (обнародования).

Глава Новотроицкого муниципального округа

Кузьменко Е. Н.



Приложение № 1
УТВЕРЖДЕНО
постановлением
Главы Новотроицкого
муниципального округа
Херсонской области
№ 800 от 24.09.2015

ПОЛИТИКА
информационной безопасности в
Администрации Новотроицкого муниципального округа
Херсонской области

1. Общие положения

1.1. Политика информационной безопасности в Администрации Новотроицкого муниципального округа Херсонской области (далее - Политика) определяет принятие правовых, организационных и технических мер, которыми руководствуется Администрация Новотроицкого муниципального округа (далее - Администрация) в своей деятельности, направленных на:

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации.

1.2. Основными составными элементами Политики являются:

защита информации при организации работ с персональными данными;

защита информации, не составляющей государственную тайну, в автоматизированных и информационных системах;

защита информации с ограниченным доступом, не составляющей государственную тайну, с использованием средств криптографической защиты информации;

защита информации, размещаемой на официальном сайте в информационно-телекоммуникационной сети Интернет.

1.3. Общее руководство обеспечением информационной безопасности в Администрации осуществляет отдел внутренней и молодежной политики Администрации. Контроль за соблюдением требований по информационной безопасности несет должностное лицо, назначенное ответственным за защиту информации.

2. Область применения

2.1. Настоящая Политика распространяется на Администрацию и обязательна к исполнению всеми ее сотрудниками.

2.2. Сотрудники обязаны соблюдать порядок обращения с конфиденциальными документами, ключевыми носителями и другой защищаемой информацией, соблюдать требования настоящей Политики и иных документов, регламентирующих деятельность в области информационной безопасности.

2.3. Действие Политики не распространяется на отношения, возникающие при обработке информации ограниченного доступа, содержащей сведения, составляющие государственную тайну. Защита информации, содержащей сведения содержащую государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

3. Термины и определения

3.1. В настоящей Политике используются следующие термины:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

Аудит информационной безопасности Администрации – процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самой Администрацией (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит);

Информационная технология – совокупность правил, приемов и методов применения средств вычислительной техники для выполнения функций хранения, обработки, передачи и использования производственной, финансовой, аналитической или иной информации, связанной с функционированием Администрации;

Информационный технологический процесс – часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования Администрации;

Информационная безопасность Администрации – состояние защищенности информационных активов Администрации в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры Администрации;

Информационные активы Администрации – активы Администрации, имеющие отношение к его информационной сфере и представляющие ценность для нее с точки зрения достижения уставных целей;

Инцидент информационной безопасности – действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов Администрации;

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их

обработку информационных технологий и технических средств в соответствии с законодательством;

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

Мониторинг информационной безопасности Администрации – постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности Администрации, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы, информационные услуги и прочее;

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем;

Политика информационной безопасности Администрации – комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых Администрацией для обеспечения информационной безопасности;

Риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы;

Роль – заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом Администрации. К субъектам относятся сотрудники Администрации, посетители, а также иницилируемые от их имени действия над объектами. Объектами являются аппаратные и программные средства, информационные ресурсы, услуги и процессы, составляющие автоматизированную систему;

Режим конфиденциальности информации – организационно-технические мероприятия по обеспечению конфиденциальности информации (защите информации), включающие в себя:

- определение перечня информации, составляющей конфиденциальную информацию;

- ограничение доступа к конфиденциальной информации путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- учет лиц, получивших доступ к конфиденциальной информации, и (или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию конфиденциальной информации работниками, на основании трудовых договоров, контрагентами, на основании гражданско-правовых договоров и соглашений, работниками со срочными трудовыми договором и проходящих в Администрации практику (стажировку);

Угроза – опасность, предполагающая возможность потери (блокирования) информации;

Управление информационной безопасностью Администрации – совокупность целенаправленных действий, осуществляемых в рамках настоящей Политики в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер – защита информации);

Уязвимость – недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Администрации при реализации угроз в информационной сфере;

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию.

4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения информационной безопасности являются:

постоянный и всесторонний анализ автоматизированных систем и информационных технологий с целью выявления уязвимостей информационных активов Администрации;

своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность, корректировка моделей угроз и нарушителя;

разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию и совместимости этих мер с действующим технологическим процессом. При этом меры, принимаемые для обеспечения информационной безопасности, не должны усложнять деятельность Администрации, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности;

контроль эффективности принимаемых защитных мер;

персонификация и адекватное разделение ролей и ответственности между сотрудниками Администрации, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5. Цели и задачи информационной безопасности

5.1. Основной целью является защита информации, содержащейся в информационных системах от наиболее распространенных угроз информационной безопасности, вызванных неэффективностью процедур контроля, технологических сбоев, несанкционированных действий сотрудников или иных форм незаконного вмешательства в информационные ресурсы и информационные системы.

5.2. Указанная цель достигается посредством обеспечения и постоянного поддержания конфиденциальности, целостности и доступности информации.

5.3. Для достижения цели защиты и обеспечения указанных свойств информации, система обеспечения информационной безопасности должна обеспечивать эффективное решение следующих задач, таких как:

оценка состояния информационной безопасности, прогнозирование и обнаружение угроз безопасности информации, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

укрепление вертикали управления и централизация сил обеспечения информационной безопасности в органе власти и местного самоуправления;

совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

обеспечение соблюдения требований законодательства Российской Федерации в области информационной безопасности;

организация и координация руководством органа власти и местного самоуправления работ по обеспечению информационной безопасности;

возложение ответственности за обеспечение безопасности информации в информационных системах на каждого сотрудника органа власти и местного самоуправления в пределах его полномочий;

обеспечение непрерывного функционирования информационных систем и системы обеспечения информационной безопасности;

обеспечение эффективной работы механизмов оперативного реагирования на компьютерные инциденты информационной безопасности;

ведение мониторинга состояния защищенности информации при ее обработке в информационных системах;

защита от вмешательства в процесс функционирования информационной системы посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных (трудовых) обязанностей), то есть защиту информации от несанкционированного доступа;

защита конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

обеспечение работоспособности криптографических средств защиты информации;

постоянный контроль выполнения требований законодательства Российской Федерации в области обеспечения информационной безопасности;

создание системы непрерывного обучения, тренировки и проверки осведомленности сотрудников по вопросам обеспечения информационной безопасности;

обеспечение защиты информации от несанкционированного доступа, предотвращение утраты, искажения или уничтожения информации на этапах

сбора, обработки, хранения и предоставления конечному потребителю информации.

5.4. Поставленные основные цели и задачи обеспечения информационной безопасности достигаются:

учетом всех подлежащих защите ресурсов информационной системы (информации, задач, документов, каналов связи, серверов, автоматизированных систем);

полнотой и непротиворечивостью требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

подготовкой сотрудников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности;

четким знанием и строгим соблюдением всеми пользователями информационной системы требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

персональной ответственностью за свои действия каждого сотрудника, имеющего доступ к информационным ресурсам, в рамках выполнения своих трудовых обязанностей;

эффективным контролем за соблюдением пользователями информационных ресурсов обязательных требований по обеспечению информационной безопасности.

6. Объекты обеспечения информационной безопасности

6.1. К объектам обеспечения информационной безопасности относятся: информационные ресурсы, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну (служебная тайна, персональные данные и другая информация ограниченного распространения), а также общедоступная (открытая) информация;

системы формирования, распространения и использования информационных ресурсов, включающие в себя информационные системы различного класса и назначения, правила и процедуры сбора, обработки, хранения и передачи информации;

информационная инфраструктура, включающая центры обработки и анализа информации, средства, системы связи и передачи данных.

6.2. В информационной системе объектами информационной безопасности 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, видео-, и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

7. Основные направления деятельности Администрации по обеспечению информационной безопасности

7.1. Деятельность по обеспечению информационной безопасности призвана способствовать снижению рисков от угроз в информационной сфере, повышению эффективности и устойчивости в управлении информационными ресурсами и системами.

К основным направлениям обеспечения информационной безопасности относятся:

правовое обеспечение информационной безопасности – деятельность направлена на создание и поддержание в актуальном состоянии системы локальных нормативных актов, регламентирующих деятельность по обеспечению информационной безопасности;

организация деятельности по обеспечению информационной безопасности

деятельность направлена на создание документированных процессов обеспечения информационной безопасности между всеми подразделениями органа власти и местного самоуправления;

обеспечение информационной безопасности при управлении информационными ресурсами – деятельность направлена на идентификацию, классификацию информационных систем и ресурсов, а также их владельцев, формирование и поддержание необходимого уровня информационной безопасности информационных ресурсов;

обеспечение информационной безопасности, связанное с сотрудниками – деятельность направлена на минимизацию рисков, вызванных действиями сотрудников в отношении информационных ресурсов, путем создания системы непрерывного обучения, тренировки и проверки осведомленности всех сотрудников по вопросам обеспечения информационной безопасности;

физическая безопасность информационных ресурсов – деятельность направлена на минимизацию и предотвращение ущерба, вызванного физическим воздействием на информационные системы и ресурсы;

обеспечение информационной безопасности на этапах жизненного цикла информации в информационной инфраструктуре – деятельность направлена на минимизацию рисков, возникающих в процессе создания, обработки, обмена и уничтожения информации в информационных системах;

управление доступом к информационным ресурсам – деятельность направлена на создание порядка доступа к информационным ресурсам, контроль и мониторинг доступа;

управление инцидентами информационной безопасности – деятельность направлена на проведение мероприятий по своевременному выявлению и реагированию на инциденты информационной безопасности;

соответствие обязательным требованиям – деятельность направлена на соответствие требованиям законодательства Российской Федерации, локальных нормативных актов по обеспечению информационной безопасности.

8. Принципы формирования системы обеспечения информационной безопасности

8.1. Построение системы обеспечения информационной безопасности и ее функционирование осуществляется в соответствии с основными принципами формирования системы обеспечения информационной безопасности.

8.2. К основным принципам формирования системы обеспечения информационной безопасности относятся:

законность — предполагает разработку системы обеспечения информационной безопасности в соответствии с действующим законодательством Российской Федерации в данной области с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Все пользователи информационных систем должны иметь представление об ответственности за правонарушения в области обеспечения информационной безопасности;

системность — предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих существенное значение для понимания и решения проблемы обеспечения информационной безопасности. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем, а также характер, возможные объекты и направления атак на них со стороны нарушителей, пути проникновения в информационные системы и несанкционированного доступа к информации;

централизация управления — предполагает, что деятельность по обеспечению информационной безопасности должна быть встроена в управленческие процессы Администрации, подчиняться понятным руководителям закономерностям и оцениваться с позиций эффективности, для этого процессы обеспечения информационной безопасности должны быть организованы и управляемы;

персональная ответственность — предполагает возложение персональной ответственности на каждого сотрудника в пределах его должностных полномочий за несоблюдение регламентирующих документов в области обеспечения информационной безопасности;

минимизация полномочий — предполагает предоставление прав доступа сотрудникам к информационным ресурсам в том случае и объеме, необходимом для качественного выполнения своих служебных (трудовых) обязанностей;

своевременность — предполагает своевременность выявления проблем, связанных с обеспечением информационной безопасности, и обнаружение угроз безопасности информации, потенциально способных нанести ущерб;

комплексный подход — предполагает всестороннее обеспечение информационной безопасности и предусматривает использование взаимоувязанных программно-технических, организационных, правовых мер обеспечения информационной безопасности на единой концептуальной основе;

непрерывность — предполагает непрерывный, целенаправленный процесс по выявлению угроз информационной безопасности и принятию адекватных

мер защиты руководством, подразделением безопасности и сотрудниками Администрации;

совершенствование – предполагает постоянное совершенствование мер и средств защиты информации на основе модернизации организационных и технических решений, кадрового состава, анализа функционирования информационной системы и системы ее защиты с учетом изменений в методах и средствах перехвата информации, обязательных требований по защите информации;

взаимодействие и сотрудничество – предполагает создание благоприятной атмосферы в коллективах структурных подразделений. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственных за обеспечение информационной безопасности. Все сотрудники должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе;

гибкость системы защиты – система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Администрацией своих полномочий. В число таких изменений входят изменения организационной и штатной структуры; изменение существующих или внедрение принципиально новых информационных систем, технических средств;

обоснованность и техническая реализуемость – информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по информационной безопасности;

обязательность контроля – предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности. Выявленные недостатки системы обеспечения информационной безопасности должны немедленно доводиться до сведения руководителя Администрации, а также оперативно устраняться.

9. Модели угроз

9.1. Модели угроз являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности Администрации.

9.2 Источники угроз, уязвимости и объекты нападений, пригодные для реализации уязвимости, типы возможных потерь, масштабы потенциального ущерба определяются документом «Модели угроз и нарушителя».

10. Требования по обеспечению информационной безопасности

10.1. Обеспечение безопасности информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы.

10.2. В качестве методов защиты информации применяются:

- правовые (законодательные) меры;
- технические меры и средства, в том числе программные средства;
- организационные меры;
- физические и иные меры.

11. Регламентация доступа в служебные помещения Администрации

11.1. Регламентация доступа в служебные помещения осуществляется в целях обеспечения физической сохранности носителей информации, оборудования и исключения возможности несанкционированного доступа в служебные помещения, в том числе, в которых ведется обработка конфиденциальной информации.

12. Разграничение доступа к техническим средствам и информационным ресурсам Администрации

12.1. Разграничение доступа к техническим средствам и информационным ресурсам направлено на предотвращение получения информации, обрабатываемой в электронном виде, в том числе в информационных системах, с нарушением регламентируемых нормативными правовыми актами или владельцами информации правил, следствием которых может быть нарушение конфиденциальности, целостности и (или) доступности информации.

12.2. Для работы с информационными ресурсами сотруднику предоставляется автоматизированное рабочее место (далее — АРМ). Программное обеспечение устанавливается и обновляется системным администратором со специальных ресурсов или съемных носителей в соответствии с лицензионным соглашением. При передаче АРМ другому сотруднику производится удаление профиля пользователя АРМ.

12.3. Для обеспечения безопасности информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;
- разработка системы защиты информации информационной системы;
- внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

12.4. К работе с информационными ресурсами допускаются сотрудники, ознакомленные с настоящей Политикой. Для осуществления доступа к информационным ресурсам сотруднику создается учетная запись – присваивается уникальный идентификатор (имя, логин) и пароль доступа. При увольнении учетная запись служащего блокируется.

13. Применение антивирусной защиты

13.1. Антивирусная защита применяется с целью защиты информационных ресурсов и программного обеспечения (далее – ПО) от несанкционированных действий (утраты, модификации, изменения) путем внедрения в информационную среду вирусов, вредоносных программ (далее – вирус) посредством использования, специализированного ПО (далее – антивирусное ПО).

13.2. Антивирусное ПО должно быть развернуто на всех технических средствах, подверженных воздействию вирусов (АРМ, серверах). Антивирусные механизмы должны быть актуальными, постоянно включенными. Должны вестись журналы протоколирования событий. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается.

14. Применение криптографической защиты информации

14.1. Криптографическая защита информации (шифрование) применяется для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении, создания электронной подписи, проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи.

15. Регламентация использования электронной почты

15.1. Система электронной почты используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов вирусами.

15.2. Угрозы, связанные с электронной почтой:

возможность создания писем с фальшивыми адресами;
 возможность нарушения конфиденциальности электронных писем;
 возможность изменения в процессе передачи содержимого электронных писем;

осуществление сетевых атак посредством отправки упакованного в архив сообщения, распаковка которого приводит к выводу системы из строя, заражению вирусами;

получение спама.

15.3. Отправка, получение официальных запросов и ответов в целях исполнения своих функций осуществляется с использованием официальных адресов электронной почты.

15.4. Перечень официальных адресов электронной почты структурных подразделений Администрации утверждается Администрацией Херсонской области.

15.5. Официальный адрес электронной почты размещается на официальном сайте Администрации в информационно-телекоммуникационной сети Интернет.

15.6. Начальник отдела внутренней и молодежной политики Администрации определяет специалистов, ответственных за работу с официальной электронной почтой.

15.7. Отправка, получение электронных сообщений в целях исполнения должностных обязанностей сотрудником осуществляется с использованием индивидуального электронного адреса сотрудника.

15.8. При увольнении сотрудника электронный почтовый ящик отключается с последующим автоматическим удалением.

15.9. При работе с электронной почтой сотрудники обязаны:
 передотправкой тщательно проверять сообщения на отсутствие информации ограниченного доступа;

периодически удалять из электронного почтового ящика ненужные сообщения и перемещать необходимые сообщения в архивные почтовые папки;
 проверять сообщения электронной почты на наличие вирусов;
 использовать шифрование, обезличивание конфиденциальной информации при ее отправке.

15.10. При работе с электронной почтой сотруднику запрещено:
 отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации;

отправлять персональные данные без предварительного обезличивания или шифрования;

отправлять сообщения с иного электронного почтового ящика или от имени другого сотрудника без предоставления полномочий;

использовать электронную почту для создания, отправки, пересылки или хранения любых подрывных, оскорбительных, неэтичных, незаконных материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии,

терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылок или других ссылок на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

рассылать компьютерные коды, файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, вирусы или другое злонамеренное ПО, программы для осуществления несанкционированного доступа, серийные номера к программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, ссылки на указанную информацию;

перехватывать, изменять, удалять, сохранять или публиковать сообщения иных сотрудников, кроме случаев, санкционированных руководителями, или в целях администрирования систем;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО, переходить по активным ссылкам, полученным от отправителей, если имеются сомнения в надежности отправителя и (или) полученного сообщения.

15.11. Содержимое электронного почтового ящика сотрудника может быть проверено системным администратором (программистом) без предварительного уведомления сотрудника в случае подозрения на осуществление рассылки писем, содержащих вредоносное ПО, спам, информацию, распространение которой запрещено правовыми актами. Информация о выявленных нарушениях направляется сотруднику и его руководителю.

16. Регламентация работы в сети Интернет

16.1. Сеть Интернет используется сотрудниками для получения информации в рамках исполнения должностных обязанностей.

16.2. Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов вирусами.

16.3. Доступ к сети Интернет предоставляется сотруднику с АРМ, закрепленного за сотрудником для исполнения должностных обязанностей, с использованием учетной записи служащего.

16.4. Угрозы, связанные с работой в сети Интернет:

легкость перехвата данных и фальсификации IP-адресов в сети Интернет; заражение вирусами.

16.5. Сотрудникам запрещается:

осуществлять действия, запрещенные законодательством Российской Федерации;

отправлять конфиденциальную информацию без предварительного шифрования криптографическим ПО, разрешенным к использованию в Администрации;

распространять информацию, содержащую подрывные, оскорбительные, неэтичные, незаконные материалы, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылки или другие ссылки на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети Интернет;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО;

открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами.

16.6. Сотрудники обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить системному администратору (ответственному по защите информации).

16.7. Вся информация об информационных ресурсах, посещаемых служащим, автоматически протоколируется и при необходимости представляется системным администратором (программистом) управляющему делами Администрации.

16.8. Доступ к сети Интернет может быть заблокирован системным администратором (программистом) без предварительного уведомления сотрудника при возникновении угрозы безопасности информации.

17. Регламентация создания и эксплуатации информационных систем

17.1. Для проведения работ по обеспечению безопасности информации в ходе создания и эксплуатации информационной системы владельцем информации (заказчиком) в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

17.2. Срок начала эксплуатации системы не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о вводе системы в эксплуатацию.

17.3. Пользователи осуществляют эксплуатацию системы в соответствии с рабочей документацией.

18. Ответственные за обеспечение информационной безопасности

18.1. Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Администрации Новотроицкого муниципального округа Херсонской области назначается сотрудник, ответственный за обеспечение информационной безопасности.

18.2. На сотрудника, ответственного за обеспечение информационной безопасности, возлагается решение следующих основных задач:
 анализ текущего состояния обеспечения информационной безопасности;
 организация мероприятий и координация работ по обеспечению информационной безопасности;
 контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

18.3. Основные функции сотрудника, ответственного за обеспечение информационной безопасности:

- формирование требований к системе обеспечения информационной безопасности в процессе создания и дальнейшего развития существующих компонентов информационной системы;

- участие в проектировании системы обеспечения информационной безопасности, ее испытаниях и вводе в эксплуатацию;

- обеспечение функционирования системы защиты информации и ее элементов, включая управление криптографическими системами;

- обучение пользователей и обслуживающего персонала правилам обработки информации;

- оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;

- контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с конфиденциальной информацией;

- организация по указанию руководства служебного расследования по фактам нарушения правил обращения с конфиденциальной информацией и оборудованием;

- принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;

- участие в работе по выявлению и устранению компьютерных инцидентов информационной безопасности.

19. Основные организационные, технические и правовые меры обеспечения безопасности информации

19.1. Для организации и внедрения системы защиты информации в информационной инфраструктуре Администрации важное значение имеет анализ технических, структурных, эксплуатационных и иных особенностей информационных систем, используемых технологий и архитектурных решений.

20. Правовые (законодательные) меры обеспечения безопасности информационных систем

20.1. К правовым (законодательным) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации нормативно-правовые акты, регламентирующие правила обращения с

информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения принятых в них правил.

13.2. Лица, виновные в нарушении обязательных требований по обеспечению информационной безопасности несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

13.3. Правовые меры защиты носят упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы.

21. Организационные меры обеспечения безопасности информационных систем

21.1. К организационным мерам обеспечения безопасности информационных систем относятся меры организационного характера, регламентирующие процессы функционирования информационных систем, использование их ресурсов, деятельность обслуживающего персонала, а также порядок обращения пользователей информации с информационными системами таким образом, чтобы в наибольшей степени затруднить либо исключить возможность реализации угроз информационной безопасности, снизить размер потерь в случае реализации угроз.

21.2. В целях минимизации риска неправомерного завладения информацией или совершения действий от имени другого пользователя в Администрации принята политика чистого стола и чистого экрана. Ответственными за исполнением этой политики являются все сотрудники Администрации, а контроль выполнением должны осуществлять руководители подразделения.

21.3. При работе с документами, распечатанными на бумажном носителе необходимо придерживаться следующих правил:

держат в столе только те документы, которые необходимы для работы в настоящий момент;

не оставлять документы на столе, если сотрудник выходит из-за рабочего места. Документы необходимо убирать в ящик стола или в соответствующие папки;

при работе с документами, содержащими информацию ограниченного доступа, необходимо убирать их в сейф, если сотрудник отходит от рабочего места.

21.4. При работе с документами в электронном виде необходимо придерживаться следующих правил:

всегда блокировать (Win+L) рабочий стол при выходе из-за рабочего места даже на непродолжительное время;

устанавливать монитор таким образом, чтобы его изображение не было видно от входной двери;

установить автоматическую блокировку экрана через 10 минут простоя (установив хранитель экрана (Screen Saver) и поставить галочку «Запрашивать пароль» или «Начинать с экрана входа в систему»);

минимизировать заполнение рабочего стола ярлыками программ и папок, не размещать документы на рабочем столе;

использовать фоны рабочего стола, содержащие общие требования (рекомендации) по информационной безопасности.

21.5. Технические меры обеспечения безопасности информационных систем. Технические меры обеспечения безопасности информационных систем должны быть основаны на использовании единых программных и технических средств, входящих в состав информационных систем и выполняющих самостоятельно или в комплексе с другими средствами функции защиты.

21.6. Технические меры обеспечения безопасности информационных систем реализуются, в том числе посредством применения средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации. Данный перечень размещен на официальном сайте Федеральной службы по техническому и экспортному контролю России (www.fstec.ru).

21.7. Применение организационных и технических мер защиты информации, реализуемых в информационных системах в рамках их систем защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

идентификацию и аутентификацию субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защиту машинных носителей информации;

регистрацию событий безопасности;

антивирусную защиту;

обнаружение вторжений;

контроль (анализ) защищенности информации;

обеспечение целостности информационной системы и информации;

обеспечение доступности информации;

защиту среды виртуализации;

защиту технических средств;

защиту информационной системы, ее средств, систем связи и передачи данных, в том числе, посредством применения активных и пассивных средств защиты информации, обрабатываемой техническими средствами информационных систем и циркулирующей в помещениях объекта от утечки по техническим каналам.

21.8. Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой

информационной системой, должны быть направлены на обеспечение конфиденциальности, целостности и доступности информации.

21.9. В условиях растущего санкционного давления со стороны политических оппонентов и недружественных стран, осуществляющих контроль компаний производителей информационно-телекоммуникационного оборудования и программного обеспечения, в том числе с использованием возможностей спецслужб иностранных государств, Администрации необходимо ориентироваться на выбор отечественного программного и информационно-телекоммуникационного оборудования, соответствующего требованиям информационной безопасности, что также соответствует текущему курсу импортозамещения Правительства Российской Федерации.

22. Криптографические методы и средства защиты

22.1. Криптографические методы и средства защиты (далее - СКЗИ) используются для обеспечения информационной безопасности.

22.2. Организация системы информационной безопасности на основе инфраструктуры с использованием СКЗИ позволит решить задачи:

организации обеспечения защищенного документооборота с использованием имеющихся систем, как внутри, так и при взаимоотношениях с другими организациями. Это позволит повысить эффективность и снизить накладные расходы на администрирование системы и использовать единые стандарты защиты данных;

реализации централизованно контролируемой системы информационной безопасности, при этом гибкой и динамически управляемой;

универсализации методов обеспечения доступа пользователей и защиты для системы электронной почты, системы доступа по информационно-

телекоммуникационным сетям общего пользования и других систем с использованием уже имеющихся в этих приложениях механизмов обеспечения информационной безопасности;

использования имеющихся реализаций российских криптографических алгоритмов в операциях с сертификатами и при защите электронного документооборота.

22.3. Использование СКЗИ для обеспечения безопасности информации необходимо в случаях, если:

информация подлежит криптографической защите в соответствии с законодательством Российской Федерации;

в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью данных средств (передача информации по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче информации, содержащей сведения конфиденциального характера, по информационно-телекоммуникационным сетям общего пользования);

хранение информации на носителях, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью не криптографических методов и способов).

22.4. При применении СКЗИ требуется учитывать:

криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ;

СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ;

для обеспечения безопасности информации при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия. Перечень СКЗИ, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России.

25. Физические меры защиты

25.1. Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

25.2. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключаящими нахождение внутри контролируемой (охраняемой) зоны технических средств съема информации.

26. Порядок реагирования на компьютерные инциденты

26.1. Реагирование на компьютерные инциденты включает в себя выполнение следующих мероприятий:

фиксацию состояния и анализ объектов информационных ресурсов, вовлеченных в инцидент;

координацию деятельности по прекращению воздействия компьютерных атак, проведение которых вызвало возникновение инцидента;

фиксацию и анализ сетевого трафика, циркулирующего в информационном ресурсе, вовлеченном в инцидент;

определение причин инцидента и возможных его последствий для информационного ресурса: первичный анализ инцидента; комплексный анализ инцидента; локализацию инцидента; сбор сведений для последующего установления причин инцидента; планирование мер по ликвидации последствий инцидента; ликвидацию последствий инцидента; контроль ликвидации последствий.

26.2. Решения должны приниматься отдельно для каждого информационного ресурса, затронутого компьютерным инцидентом.

27. Обучение сотрудников и повышение осведомленности в вопросах обеспечения информационной безопасности

27.1. Все пользователи информационной системы должны быть ознакомлены с организационно-распорядительными документами по обеспечению информационной безопасности, в части, их касающейся, должны знать и неукоснительно выполнять инструкции, и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, осуществляется под подпись. Пользователи информационной системы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки конфиденциальной информации.

27.2. Целью обучения сотрудников является, снижение потерь (материальных, финансовых, ущерб репутации и т.д.) от угроз, связанных с незнанием или непониманием основных положений законодательства Российской Федерации в области обеспечения информационной безопасности и правил по защите информации.

27.3. Задачи повышения осведомленности сотрудников в вопросах информационной безопасности:

- информирование сотрудников о существующих угрозах и проблемах информационной безопасности, которые могут возникнуть при автоматизированной обработке информации, обновление их теоретических и практических знаний в области обеспечения информационной безопасности;

- доведение до сотрудников основных положений, ограничений и требований существующих нормативно-распорядительных документов, принятых в Администрации;

- выработка у сотрудников умения оценивать возможные последствия своих действий (адекватно оценивать связанные с ними риски информационной безопасности);

- выработка у сотрудников привычек, способствующих поддержанию высокого уровня информационной безопасности;

- выработка у сотрудников Администрации умений (навыков) правильно и оперативно действовать при возникновении инцидентов информационной безопасности;

доведение до сотрудников их обязанностей в области обеспечения информационной безопасности и степени их ответственности в случае утечки конфиденциальной информации;

оценка эффективности, развитие и совершенствование проводимых мероприятий по информационной безопасности в целом.

27.4. Формы и методы повышения осведомленности сотрудников в области информационной безопасности:

инструктаж при приеме на работу;

повышение квалификации (курсы, семинары, тренинги);

дистанционное обучение;

инструктажи и зачеты по положениям законодательства Российской Федерации в области обеспечения информационной безопасности и настоящей Политики.

28. Контроль состояния информационной безопасности

28.1. Контроль состояния информационной безопасности осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

28.2. Основная задача контроля заключается в получении объективных оценок текущего состояния обеспечения информационной безопасности, оценка эффективности применяемых мер и технических решений для обеспечения информационной безопасности, оказание методической помощи по обеспечению защиты информации, организация работы по обеспечению информационной безопасности.

28.3. Контроль проводится сотрудником обеспечения информационной безопасности и комиссией, назначаемой для этой цели.

28.4. Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Приложение № 2
УТВЕРЖДЕНО
постановлением
Главы Новотроицкого
муниципального округа
Херсонской области
№ 800 от 24.09.2025

ПОЛИТИКА
обработки персональных данных в
Администрации Новотроицкого муниципального округа
Херсонской области

1. Общие положения

1.1. Настоящая Политика обработки персональных данных в Администрации Новотроицкого муниципального округа Херсонской области (далее - Политика) разработана во исполнение требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных) в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика действует в отношении всех персональных данных, которые обрабатывает Администрация Новотроицкого муниципального округа Херсонской области (далее - Оператор).

1.3. Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных настоящая Политика публикуется в свободном доступе в информационно-телекоммуникационной сети Интернет на сайте Оператора.

1.5. Основные понятия, используемые в Политике:

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

оператор 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;

обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования.

Обработка персональных данных включает в себя в том числе:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение;

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.

1.6. Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, ответственным за организацию обработки персональных данных у Оператора.

1.7. Ответственность за нарушение требований законодательства Российской Федерации и нормативных актов Администрацией Новотроицкого муниципального округа Херсонской области в сфере обработки и защиты

персональных данных определяется в соответствии с законодательством Российской Федерации.

2. Права и обязанности Оператора

2.1. Оператор имеет право:

получать от субъекта персональных данных достоверную информацию и (или) документы, содержащие персональные данные для осуществления целей обработки;

самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;

поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных;

в случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных;

2.2. Оператор обязан:

организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;

отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;

по запросу субъекта персональных данных предоставлять ему информацию, предусмотренную частью 7 статьи 14 Федерального закона № 152-ФЗ «О персональных данных», включая сведения о факте обработки, правовых основаниях, целях, источнике и сроках обработки его персональных данных, а также иную информацию, установленную законом;

сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)) по запросу этого органа необходимую информацию в течение 30 дней с даты получения такого запроса.

3. Права субъекта персональных данных

3.1. Субъект персональных данных имеет право:

получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;

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

выдвигать условие предварительного согласия при обработке персональных данных в целях продвижения на рынке товаров, работ и услуг;

обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных;

в любой момент отозвать согласие на обработку своих персональных данных посредством письменного обращения к оператору. В случае отзыва согласия обработка прекращается, если иное не предусмотрено федеральным законом.

4. Цели сбора персональных данных

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

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

4.3. Обработка Оператором персональных данных осуществляется в следующих целях:

обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;

обеспечение соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;

обеспечение соблюдения трудового законодательства Российской Федерации;

обеспечение соблюдения налогового законодательства Российской Федерации;

обеспечение соблюдения пенсионного законодательства Российской Федерации;

обеспечение соблюдения законодательства о муниципальной службе в Российской Федерации;

обеспечение соблюдения жилищного законодательства Российской Федерации;

обеспечение соблюдения законодательства Российской Федерации о противодействии терроризму;

обеспечение соблюдения законодательства Российской Федерации о безопасности;

обеспечение соблюдения законодательства Российской Федерации о противодействии коррупции;

заключение и выполнение обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами, в том числе подготовка, заключение и исполнение гражданско-правового договора;

обеспечение пропускного режима на территорию Оператора;

обеспечение прохождения ознакомительной, производственной или преддипломной практики на основании договора с учебным заведением;

ведение кадрового учета, в том числе выполнение требований трудового законодательства о муниципальной службе в части ведения кадрового учета;

ведение кадрового делопроизводства, в том числе подбор персонала (соискателей) на вакантные должности Оператора;

ведение воинского учета;

ведение бухгалтерского учета;

формирование кадрового резерва;

оформление договорных отношений в соответствии с законодательством Российской Федерации;

ведение личных дел (карточек);

представление граждан к награждениям;

регистрация и обработка сведений, необходимых для реализации полномочий Администрации Новотроицкого муниципального округа Херсонской области;

рассмотрение обращений граждан, подготовка ответов на обращения;

ведение официального сайта Администрации Новотроицкого муниципального округа Херсонской области;

осуществление и выполнение возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

оказание муниципальных услуг;

осуществление своей деятельности в соответствии с Уставом Администрации Новотроицкого муниципального округа Херсонской области;

выполнение иных уставных задач.

4.4. Обработка персональных данных работников может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.

5. Правовые основания обработки персональных данных

5.1. Правовым основанием обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, в том числе:

Конституция Российской Федерации;
Гражданский кодекс Российской Федерации;
Трудовой кодекс Российской Федерации;
Налоговый кодекс Российской Федерации;
Федеральный закон от 06.12.2011 № 402-ФЗ "О бухгалтерском учете";
Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных";
иные нормативные правовые акты, регулирующие отношения, связанные с деятельностью Оператора.

5.2. Правовым основанием обработки персональных данных также являются:

Устав муниципального образования Новотроицкого муниципального округа Херсонской области;

договоры, заключаемые между Оператором и субъектами персональных данных;

согласие субъектов персональных данных на обработку их персональных данных.

6. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

6.1. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, предусмотренным в разд. 2 настоящей Политики. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6.2. Оператор может обрабатывать персональные данные следующих категорий субъектов персональных данных.

6.2.1. Кандидаты для приема на работу к Оператору:

фамилия, имя, отчество;

пол;

гражданство;

дата и место рождения;

контактные данные;

сведения об образовании, опыте работы, квалификации;

иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

6.2.2. Работники и бывшие работники Оператора:

фамилия, имя, отчество;

пол;

гражданство;

дата и место рождения;

изображение (фотография);

паспортные данные;
 адрес регистрации по месту жительства;
 адрес фактического проживания;
 контактные данные;
 индивидуальный номер налогоплательщика;
 страховой номер индивидуального лицевого счета (СНИЛС);
 сведения об образовании, квалификации, профессиональной подготовке и
 повышении квалификации;
 семейное положение, наличие детей, родственные связи;
 сведения о трудовой деятельности, в том числе наличие поощрений,
 наград и (или) дисциплинарных взысканий;
 данные о регистрации брака;
 сведения о воинском учете;
 сведения об инвалидности;
 сведения об удержании алиментов;
 сведения о доходе с предыдущего места работы;
 иные персональные данные, предоставляемые работниками в
 соответствии с требованиями трудового законодательства.

6.2.3. Члены семьи работников Оператора:

фамилия, имя, отчество;
 степень родства;
 год рождения;
 иные персональные данные, предоставляемые работниками в
 соответствии с требованиями трудового законодательства.

6.2.4. Клиенты и контрагенты Оператора (физические лица):

фамилия, имя, отчество;
 дата и место рождения;
 паспортные данные;
 адрес регистрации по месту жительства;
 контактные данные;
 замещаемая должность;
 индивидуальный номер налогоплательщика;
 номер расчетного счета;
 иные персональные данные, предоставляемые клиентами и
 контрагентами (физическими лицами), необходимые для заключения и
 исполнения договоров.

6.2.5. Представители (работники) клиентов и контрагентов Оператора (юридических лиц):

фамилия, имя, отчество;
 паспортные данные;
 контактные данные;
 замещаемая должность;
 иные персональные данные, предоставляемые представителями
 (работниками) клиентов и контрагентов, необходимые для заключения и
 исполнения договоров.

6.2.6. Лица, которые обращаются с заявлениями, письмами, жалобами:
 фамилия, имя, отчество;
 дата и место рождения;
 адрес регистрации по месту жительства;
 контактные данные.

6.3. Оператором не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

7. Порядок и условия обработки персональных данных

7.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

7.2. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

7.3. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

7.4. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

7.5. Обработка персональных данных осуществляется путем:
 получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных;
 получения персональных данных из общедоступных источников;
 внесения персональных данных в журналы, реестры и информационные системы Оператора;
 использования иных способов обработки персональных данных.

7.6. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

7.7. Передача персональных данных органам дознания и следствия, в Федеральную налоговую службу, Пенсионный фонд Российской Федерации, Фонд социального страхования и другие уполномоченные органы исполнительной власти и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

7.8. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или

случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

определяет угрозы безопасности персональных данных при их обработке;
принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;
назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора;

создает необходимые условия для работы с персональными данными;
организует учет документов, содержащих персональные данные;
организует работу с информационными системами, в которых обрабатываются персональные данные;

хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

организует обучение работников Оператора, осуществляющих обработку персональных данных.

7.9. Оператор осуществляет хранение персональных данных 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.

7.10. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, Оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в Законе о персональных данных.

8. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

8.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Оператором субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя.

8.2. В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

8.3. Запрос должен содержать:

номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором; подпись субъекта персональных данных или его представителя.

8.4. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.5. Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

8.6. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

8.7. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

8.8. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

8.9. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

8.10. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

8.11. В случае получения письменного отзыва согласия на обработку персональных данных Оператор прекращает обработку таких данных и уничтожает их либо блокирует, если хранение данных требуется федеральным законом, кроме случаев, когда оператор имеет право обрабатывать данные без согласия субъекта (пункты 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ).

9. Заключительные положения

9.1. Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

9.2. Настоящая Политика является внутренним документом Оператора, и является общедоступной и размещается на официальных сайтах Администрации Новотроицкого муниципального округа Херсонской области в информационно-телекоммуникационной сети «Интернет» по адресам:

<https://novotroick-r74.gosweb.gosuslugi.ru>

<https://novotroitskoe.gosuslugi.ru>

9.3. Администрация Новотроицкого муниципального округа Херсонской области оставляет за собой право вносить необходимые изменения в Политику при изменении действующего законодательства Российской Федерации и условий своей деятельности. Изменения в Политику размещаются на официальном сайте Администрации Новотроицкого муниципального округа Херсонской области.

Приложение № 3
УТВЕРЖДЕНО
постановлением
Главы Новотроицкого
муниципального округа
Херсонской области
№ 800 от 24.09.2015

ПОЛИТИКА
обработки персональных данных на официальных сайтах
Администрации Новотроицкого муниципального округа
Херсонской области

1. Общие положения

1. Общие положения

Настоящая политика обработки персональных данных на официальных сайтах Администрации Новотроицкого муниципального округа Херсонской области (далее — Политика) составлена в соответствии с требованиями Федерального закона от 27.07.2006. №152-ФЗ «О персональных данных» (далее - Закон о персональных данных) и определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных, предпринимаемые Оператором.

1.1. Оператор ставит своей важнейшей целью и условием осуществления своей деятельности соблюдение прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Политика применяется ко всей информации, которую Оператор может получить о посетителях веб-сайтов <https://novotroick-r74.gosweb.gosuslugi.ru> и <https://novotroitskoe.gosuslugi.ru> (далее — веб-сайт).

2. Основные понятия

2.1. Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

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

2.3. Веб-сайты — совокупность графических и информационных материалов, а также программ для ЭВМ и баз данных, обеспечивающих их доступность в сети интернет по сетевым адресам <https://novotroick-r74.gosweb.gosuslugi.ru> и <https://novotroitskoe.gosuslugi.ru>.

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

2.5. **Обезличивание персональных данных** — действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному Пользователю или иному субъекту персональных данных.

2.6. **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.

2.7. **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.

2.8. **Персональные данные** — любая информация, относящаяся прямо или косвенно к определенному или определяемому Пользователю веб-сайта.

2.9. **Персональные данные, разрешенные субъектом персональных данных для распространения**, — персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Законом о персональных данных (далее — персональные данные, разрешенные для распространения).

2.10. **Пользователь** — любой посетитель веб-сайта.

2.11. **Предоставление персональных данных** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.12. **Распространение персональных данных** — любые действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.13. **Уничтожение персональных данных** — любые действия, в результате которых персональные данные уничтожаются безвозвратно с невозможностью дальнейшего восстановления содержания персональных данных в информационной системе персональных данных и (или) уничтожаются материальные носители персональных данных.

3. Права и обязанности Оператора

3.1. Оператор имеет право:

получать от субъекта персональных данных достоверные информацию и/или документы, содержащие персональные данные;

в случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных;

самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами.

3.2. Оператор обязан:

предоставлять субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных;

организовывать обработку персональных данных в порядке, установленном действующим законодательством РФ;

отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;

сообщать в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 дней с даты получения такого запроса;

публиковать или иным образом обеспечивать неограниченный доступ к настоящей Политике в отношении обработки персональных данных;

принимать правовые, организационные и технические меры 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;

прекратить передачу (распространение, предоставление, доступ) персональных данных, прекратить обработку и уничтожить персональные данные в порядке и случаях, предусмотренных Законом о персональных данных;

исполнять иные обязанности, предусмотренные Законом о персональных данных.

4. Основные права и обязанности Пользователя

4.1. Пользователь имеет право:

получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением

случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных;

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

на отзыв согласия на обработку персональных данных;

обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействие Оператора при обработке его персональных данных;

на осуществление иных прав, предусмотренных законодательством РФ.

4.2. Пользователь обязан:

предоставлять Оператору достоверные данные о себе;

сообщать Оператору об уточнении (обновлении, изменении) своих персональных данных.

4.3. Лица, передавшие Оператору недостоверные сведения о себе, либо сведения о другом субъекте персональных данных без согласия последнего, несут ответственность в соответствии с законодательством РФ.

5. Персональные данные Пользователя, подлежащие обработке Оператором

5.1. Оператор может обрабатывать следующие персональные данные Пользователя:

фамилия, имя, отчество;

электронный адрес;

обезличенных данных о посетителях (в т.ч. файлов «cookie») с помощью сервисов интернет-статистики (Яндекс Метрика и других).

5.2. Вышеперечисленные данные далее по тексту Политики объединены общим понятием Персональные данные.

6. Принципы обработки персональных данных

6.1. Обработка персональных данных осуществляется на законной и справедливой основе.

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

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

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

6.5. Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки.

6.6. При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор принимает необходимые меры и/или обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

6.7. Хранение персональных данных осуществляется 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 уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7. Цели обработки персональных данных

7.1. Цель обработки персональных данных Пользователя: информирование Пользователя посредством отправки электронных писем;

предоставление доступа Пользователю к сервисам, информации и/или материалам, содержащимся на веб-сайте <https://sharypovo.gosuslugi.ru>.

7.2. Обезличенные данные Пользователей, собираемые с помощью сервисов интернет-статистики, служат для сбора информации о действиях Пользователей на сайте, улучшения качества сайта и его содержания.

8. Правовые основания обработки персональных данных

8.1. Правовыми основаниями обработки персональных данных Оператором являются:

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ;

Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ;

Устав муниципального образования Новотроицкого муниципального округа Херсонской области;

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178;

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 №180;

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.11.2022 №187;

согласие Пользователей на обработку их персональных данных.

8.2. Оператор обрабатывает персональные данные Пользователя в случае их заполнения и/или отправки Пользователем самостоятельно через специальные формы (при их наличии), расположенные на веб-сайтах или направленные Оператору посредством электронной почты, а также в случаях, установленных законодательством Российской Федерации. Заполняя соответствующие формы и/или отправляя свои персональные данные Оператору, Пользователь выражает свое согласие с данной Политикой.

8.3. Оператор обрабатывает обезличенные данные о Пользователе в случае, если это разрешено в настройках браузера Пользователя (включено сохранение файлов «cookie» и использование технологии JavaScript).

8.4. Субъект персональных данных самостоятельно принимает решение о предоставлении его персональных данных и дает согласие свободно, своей волей и в своем интересе.

9. Условия обработки персональных данных

9.1. Обработка персональных данных осуществляется в следующих случаях:

9.1.1. обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

9.1.2. обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

9.1.3. обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

9.1.4. обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по

которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных;

9.1.5. обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 настоящего Федерального закона, при условии обязательного обезличивания персональных данных;

9.1.6. обработка персональных данных, полученных в результате обезличивания персональных данных, осуществляется в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных Федеральным законом от 24 апреля 2020 года N 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных" и Федеральным законом от 31 июля 2020 года N 258-ФЗ "Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации", в порядке и на условиях, которые предусмотрены указанными федеральными законами;

9.1.7. осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

10. Порядок сбора, хранения, передачи и других видов обработки персональных данных

10.1. Безопасность персональных данных, которые обрабатываются Оператором, обеспечивается путем реализации правовых, организационных и технических мер, необходимых для выполнения в полном объеме требований действующего законодательства в области защиты персональных данных.

10.2. Оператор обеспечивает сохранность персональных данных и принимает все возможные меры, исключающие доступ к персональным данным неуполномоченных лиц.

10.3. Персональные данные Пользователя не передаются третьим лицам, за исключением случаев, связанных с исполнением действующего законодательства либо в случае, если субъектом персональных данных дано согласие Оператору на передачу данных третьему лицу для исполнения обязательств по гражданско-правовому договору.

10.4. В случае выявления неточностей в персональных данных, Пользователь может актуализировать их самостоятельно, путем направления Оператору уведомления на адрес электронной почты Оператора

Novotroitsk_admin@khogov.ru с пометкой «Актуализация персональных данных».

10.5. Срок обработки персональных данных определяется достижением целей, для которых были собраны персональные данные, если иной срок не предусмотрен договором или действующим законодательством.

Пользователь может в любой момент отозвать свое согласие на обработку персональных данных, направив Оператору уведомление посредством электронной почты на электронный адрес Оператора Novotroitsk_admin@khogov.ru с пометкой «Отзыв согласия на обработку персональных данных».

10.6. Вся информация, которая собирается сторонними сервисами, в том числе средствами связи и другими поставщиками услуг, хранится и обрабатывается указанными лицами (Операторами) в соответствии с их Пользовательским соглашением и Политикой конфиденциальности. Субъект персональных данных и/или Пользователь обязан самостоятельно своевременно ознакомиться с указанными документами. Оператор не несет ответственность за действия третьих лиц, в том числе указанных в настоящем пункте поставщиков услуг.

10.7. Установленные субъектом персональных данных запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных для распространения, не действуют в случаях обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством РФ.

10.8. Оператор при обработке персональных данных обеспечивает конфиденциальность персональных данных.

10.9. Оператор осуществляет хранение персональных данных 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.

10.9. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия субъекта персональных данных или отзыв согласия субъектом персональных данных, а также выявление неправомерной обработки персональных данных.

11. Перечень действий, производимых Оператором с полученными персональными данными

11.1. Оператор осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

11.2. Оператор осуществляет автоматизированную обработку персональных данных с получением и/или передачей полученной информации по информационно-телекоммуникационным сетям или без таковой.

12. Конфиденциальность персональных данных

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

13. Заключительные положения

13.1. Пользователь может получить любые разъяснения по интересующим вопросам, касающимся обработки его персональных данных, обратившись к Оператору с помощью электронной почты Novotroitsk_admin@khogov.ru.

13.2. В данном документе будут отражены любые изменения политики обработки персональных данных Оператором. Политика действует бессрочно до замены ее новой версией.

13.3. Актуальная версия Политики в свободном доступе расположена в сети Интернет по сетевым адресам <https://novotroick-r74.gosweb.gosuslugi.ru> и <https://novotroitskoe.gosuslugi.ru>.