**ПОЛИТИКА БЕЗОПАСНОСТИ САЙТА https://kostroma.santehnic-doma.ru/**

Настоящая стандартизированная политика безопасности (далее – Политика безопасности) действует в отношении всех персональных данных, полученных от субъекта персональных данных (далее по тексту – «Пользователя») или его представителя, которую сайт в информационно-телекоммуникационной сети Интернет, расположенный на доменном имени https://kostroma.santehnic-doma.ru/ (далее по тексту – «Сайт»), принадлежащий администрации сайта (далее по тексту – «Оператор»), может получить о Пользователе во время использования Сайта, его программ и продуктов.

1. При обработке персональных данных Пользователя Оператор принимает необходимые правовые, организационные и технические меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом РФ № 152-ФЗ от 27.07.2006 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, а также 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.
2. К таким мерам, в частности, относятся:
3. изданием настоящей Политики безопасности и опубликованием ее информационно-телекоммуникационной сети Интернет на своем Сайте;
4. доведением до неопределенного круга лиц информации об Операторе, содержащей его наименование, основной государственный регистрационный номер налогоплательщика, идентификационный номер налогоплательщика, место нахождения (адрес), адрес электронной почты;
5. установлением стандартизированного Согласия на обработку персональных данным физическим лицом;
6. назначение Оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;
7. ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, установленных локальными документами Оператора;
8. установлением типовой формы согласия работников Оператора на обработку персональных данных;
9. установлением типового обязательства работника Оператора, осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением трудовых обязанностей;
10. организацией обучения работников Оператора, обрабатывающих персональные данные;
11. установлением правил обработки персональных данных, устанавливающих процедуры, направленные на выявление и предотвращение нарушений [законодательства](http://base.garant.ru/12148567/1/#block_4) РФ в сфере персональных данных, а также определяющих для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории Пользователей, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;
12. установлением правил рассмотрения запросов Пользователя или его представителя;
13. установлением правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральными законами, принятыми в соответствии с ним нормативными правовыми актами и локальными актами Оператора;
14. установлением правил работы с обезличенными данными в случае обезличивания персональных данных;
15. установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
16. определением перечней информационных систем персональных данных;
17. определением перечня персональных данных, обрабатываемых Оператором;
18. установлением должностных обязанностей или должностных инструкций лица, ответственного за организацию обработки персональных данных, и работников Оператора, осуществляющих обработку персональных данных;
19. установлением порядка доступа работников Оператора в помещения, в которых ведется обработка персональных данных;
20. установлением организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
21. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
22. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
23. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
24. оценкой вреда, который может быть причинен Пользователю в случае нарушения требований в области защиты персональных данных;
25. учетом машинных носителей персональных данных;
26. проверками и обеспечением технической укрепленности помещений, в которых обрабатываются персональные данные, хранится относящаяся к их обработке документация;
27. обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
28. сообщением в правоохранительные органы о фактах несанкционированного доступа к персональным данным;
29. восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
30. проведением периодических проверок условий обработки персональных данных ответственным за организацию обработки персональных данных лицом либо комиссией, образуемой Оператором;
31. осуществлением внутреннего контроля и (или) аудита соответствия обработки персональных данных федеральным законам и принятым в соответствии с ними нормативными правовыми актами, требованиям к защите персональных данных, Политике безопасности Оператора в отношении обработки персональных данных, локальным актам Оператора;
32. уведомлением уполномоченного органа по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных федеральными законами;
33. представлением документов и локальных актов Оператора и (или) иным образом подтверждением принятие мер по защите персональных данных уполномоченному органу по защите прав субъектов персональных данных.