УТВЕРЖДЕНО  
приказом Росжелдора  
от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_

**Инструкция пользователя  
государственной информационной системы персональных данных**

**Федерального агентства железнодорожного транспорта**

1. **Общие положения**
   1. Пользователь, обрабатывающий персональные данные (далее – Пользователь), осуществляет обработку персональных данных в государственной информационной системе Федерального агентства железнодорожного транспорта (Росжелдор), обрабатывающей персональные данные.
   2. Пользователем является каждый государственный служащий Росжелдора, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, персональным данным и средствам защиты информации.
   3. Пользователь несет персональную ответственность за свои действия.
   4. Пользователь в своей работе руководствуется настоящей инструкцией, политикой в отношении обработки персональных данных и другими локальными актами Росжелдора по обеспечению защиты персональных данных, а также руководящими и нормативными документами ФСТЭК России.
   5. Методическое руководство по работе пользователя (в части информационной безопасности) осуществляется администратором информационной безопасности.
2. **Должностные обязанности Пользователя**
   1. Пользователь обязан:
      1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних локальных актов Росжелдора по защите персональных данных.
      2. Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него в Перечне лиц, допущенных к автоматизированной обработке персональных данных, обрабатываемых в государственных информационных системах Федерального агентства железнодорожного транспорта.
      3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету и хранению персональных данных, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.
      4. Соблюдать инструкции антивирусной и парольной защиты.
      5. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, жалюзи на окнах должны быть закрыты.
      6. Обо всех выявленных нарушениях, связанных с информационной безопасностью в Росжелдоре, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к администратору информационной безопасности.
      7. Для получения консультаций по вопросам работы и настройке элементов государственных информационных систем, обрабатывающих персональные данные, необходимо обращаться к администратору данных систем.
      8. При отсутствии визуального контроля над автоматизированным рабочим местом, доступ к компьютеру должен быть немедленно заблокирован.
      9. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.
   2. Пользователям запрещается:
      * 1. Разглашать защищаемую информацию третьим лицам.
        2. Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.
        3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
        4. Несанкционированно открывать общий доступ к папкам на своем рабочем месте.
        5. Подключать к автоматизированному рабочему месту и корпоративной информационной сети личные внешние носители и мобильные устройства.
        6. Отключать (блокировать) средства защиты информации.
        7. Обрабатывать на автоматизированном рабочем месте информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к персональным данным.
        8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам государственных информационных систем, обрабатывающих персональные данные.
        9. Привлекать посторонних лиц для производства ремонта или настройки автоматизированного рабочего места, без согласования администратора информационной безопасности.