УТВЕРЖДАЮ
Директор ГБУ СО ЯО
Краснoперекопский
психоневрологический
интернат

_____М.В.Филиппова
«10» 01 2022 г.

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в государственном учреждении социального обслуживания Ярославской области Краснoперекопский психоневрологический интернат

1.Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 152 - ФЗ «О персональных данных» и определяет обязанности, полномочия и ответственность пользователей, допущенных к работе в информационных системах персональных данных в государственном учреждении социального обслуживания Ярославской области Краснoперекопский психоневрологический интернат (далее – учреждение).

1.2.Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационных системах персональных данных в учреждении.

1.3.Пользователем является сотрудник, допущенный к работе в информационных системах персональных данных, в соответствии с приказом директора учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, персональным данным и средствам защиты информации.

1.4.Пользователь несет персональную ответственность за свои действия.

1.5.Пользователь в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и другими внутренними нормативно-правовыми актами учреждения по защите персональных данных.

2. Обязанности пользователя

2.1.Пользователь обязан:

2.1.1. Знать и выполнять требования законодательства Российской Федерации, нормативных и руководящих документов Федеральной службы по техническому и экспортному контролю, а также внутренних документов учреждения по вопросам обработки и защиты персональных данных.

2.1.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.1.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.

2.1.4. Соблюдать требования парольной политики.

2.1.5. Соблюдать правила при работе в сетях общего доступа и международного обмена – Интернет.

2.1.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами.

2.1.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью в учреждении, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обработку персональных данных.

2.1.8. Для получения консультаций по вопросам работы и настройке элементов информационной системы персональных данных необходимо обращаться к ответственному за обработку персональных данных в информационных системах.

2.1.9. Принимать меры реагирования в случае возникновения внештатных или аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него обязанностей.

2.2. Пользователям запрещается:

2.2.1. Разглашать защищаемую информацию третьим лицам.

2.2.2. Копировать защищаемую информацию на внешние носители без письменного разрешения директора учреждения.

2.2.3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.2.4. Несанкционированно открывать общий доступ к ресурсам.

2.2.5. Запрещено подключать к АРМ и корпоративной информационной

сети личные внешние носители и мобильные устройства; отключать (блокировать) средства защиты информации, в том числе антивирусную защиту.

2.2.6. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных.

2.2.7. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системы персональных данных.

2.2.8. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным лицом.

2.3. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.4. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

3. Ответственность

3.1. Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.