МИНСОЦТРУДЗАНЯТОСТИ РЕСПУБЛИКИ МОРДОВИЯ

ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«СОЦИАЛЬНАЯ ЗАЩИТА НАСЕЛЕНИЯ ПО ИНСАРСКОМУ РАЙОНУ
РЕСПУБЛИКИ МОРДОВИЯ (МЕЖРАЙОННАЯ)»
(ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»)

П Р И К А З

17 апреля 2024 года № ОД-30

г. Инсар

Об утверждении Порядка администрирования и предоставления, прав доступа пользователей к информационным системам, сервисам и ресурсам ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»

В соответствии с положениями Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в целях обеспечения безопасности информационных систем, сервисов и ресурсов в ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)», **п р и к а з ы в а ю:**

1. Утвердить Порядок администрирования и предоставления, прав доступа пользователей к информационным системам, сервисам и ресурсам ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)» (далее – Учреждение) (Приложение № 1).

2. Специалисту по кадрам аппарата управления (Метликина М.А.):

довести настоящий приказ до сведения работников Учреждения под роспись в срок до 22.04.2024 (Приложение № 2).

3. Специалисту по социальной работе отделения дневного пребывания граждан пожилого возраста и инвалидов (Присяжнова Е.Н.) разместить настоящий приказ на официальном сайте Учреждения в разделе «Документы/Локальные нормативные акты»/ «Приказы».

4. Настоящий приказ вступает в силу с момента подписания.

Контроль за исполнением настоящего приказа оставляю за собой.

Директор С.В.Анисимова

Приложение №1
к приказу ГКУ «Соцзащита
населения по Инсарскому
району РМ (межрайонная)»
от «17» апреля 2024 №ОД-30

ПОРЯДОК

администрирования и предоставления, прав доступа пользователей к информационным системам, сервисам и ресурсам ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»

1. Общие положения

1.1. В целях обеспечения безопасности информационных систем, сервисов и ресурсов ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)» (далее - Учреждение), соблюдения принципа персональной ответственности пользователей за свои действия, авторизованный доступ пользователей к информационным системам, сервисам и ресурсам Учреждения обеспечивается на основе зарегистрированных персональных учетных записей, которые являются уникальными идентификаторами пользователей.

1.2. Под «пользователем» понимается одно физическое лицо, которому необходим доступ к определенным информационным системам, сервисам и ресурсам Учреждения.

1.3. Организационное и техническое обеспечение процессов изменения полномочий (предоставление/изменение/прекращение прав доступа) возлагается:

13.1. В информационных системах платформы «тс» «1С Предприятие», «Портал федерального казначейства», «Бюджет-WEB», «СУФД» (Система удаленного финансового документооборота для казначейства), «Сбис» (Комплексная система для корпоративного учёта и электронного документооборота), «Плагин», «bus.gov.ru», «ЕИС» (Единая информационная система в сфере закупок в информационно - телекоммуникационной сети Интернет), «WEB-Торги-КС» — на отдел бухгалтерского учета.

1.3.2. В сервисах и разделах ограниченного доступа, размещенных на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет» (insar.soc13.ru), ВКонтакте (https://m.vk.com/club217623918) — на отдел дневного пребывания граждан пожилого возраста и инвалидов.

1.3.3. В «АИС ЭСРН РМ» (Автоматизированная информационная система «Электронный социальный регистр населения Республики Мордовия), «ПГС» (Платформа государственных сервисов), «ПОС» (портал обратной связи), Сайт ФНС (Федеральная налоговая служба), ЕГИССО (Единая государственная информационная система социального обеспечения), межведомственная система электронного документооборота и автоматизированного делопроизводства

Республики Мордовия (СЭД-«Дело»), VIPNet Client (Деловая почта), РСХБ – Свой Бизнес, доступ к информационно-телекоммуникационной сети «Интернет», информационно-правовому обеспечению «Гарант», справочным ресурсам и файлообменнику - на социальную службу по выплате мер социальной поддержки.

1.3.4. Доступ к ЕИС (Единая информационная система в сфере закупок в информационно- телекоммуникационной сети Интернет), WEB-Торги-КС, Портал «Работа России» - на специалиста по кадрам аппарата управления.

1.4. Положения настоящего Порядка администрирования и предоставления, прав доступа пользователей к информационным системам, сервисам и ресурсам Учреждения (далее — Порядок) должны анализироваться специалистоми по социальной работе социальной службы по выплате мер социальной поддержки не реже одного раза в год. В случае если в ходе такого анализа была установлена необходимость внесения изменений в Порядок, новая редакция Порядка разрабатывается заведующим социальной службы по выплате мер социальной поддержки.

2. Область применения

2.1 Настоящий Порядок регламентирует действия по:

- предоставлению доступа к информационным системам, сервисам и ресурсам Учреждения;
- созданию, блокировке/аннулированию учетных записей пользователей, а также внесению изменений в разрешения учетных записей пользователей информационных систем, сервисов и ресурсов Учреждения.

2.2. Требования настоящего Порядка обязательны для выполнения всеми работниками Учреждения.

3. Требования к учетным записям пользователей и парольной защите

3.1. Не допускается создание не персонифицированных, групповых и анонимных учетных записей пользователей. Использование несколькими сотрудниками Учреждения одного и того же имени пользователя запрещено, за исключением отдельных учетных записей пользователей электронного почтового сервера Учреждения по согласованию.

3.2. Пользователи информационных систем, сервисов и ресурсов Учреждения должны осуществлять подключение к ним только с использованием собственных учетных данных для авторизации (логин и пароль). Подключение с использованием чужих учетных записей (логинов и паролей) не допускается.

3.3. При создании новой учетной записи первоначальное значение пароля устанавливается администратором соответствующей информационной системы, сервиса или ресурса, указанным в п. 1.3 настоящего Порядка.

3.4. Соответствующая информационная система, сервис или ресурс настраиваются таким образом, чтобы после первоначального входа пользователю

была предоставлена возможность установления собственного личного пароля. При отсутствии такой возможности создание/изменение личного пароля осуществляется администратором соответствующей информационной системы, сервиса или ресурса, в том числе в случае соблюдения периодичности смены личных паролей, принятых в Учреждении.

3.5.Периодичность смены паролей пользователей информационных систем, сервисов и ресурсов должна составлять не реже одного раза в 90 дней. Исключение могут составлять информационные ресурсы, где такая возможность со стороны пользователя не предусмотрена.

3.6. В целях обеспечения криптоустойчивости паролей, предотвращения возможности их угадывания либо подбора, в том числе с помощью специализированного программного обеспечения, личные пароли пользователей информационных систем, сервисов и ресурсов Учреждения должны удовлетворять следующим требованиям:

3.6.1. Длина пароля должна быть не менее 8 символов.

3.6.2. В числе символов пароля должны присутствовать три из четырех видов символов:

- буквы в верхнем регистре;
- буквы в нижнем регистре;
- цифры;
- специальные символы (! @ $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , .

3.6.3. Пароль не должен содержать легко вычисляемые сочетания символов, например:

- собственные имена, фамилии, номера телефонов, даты;
- последовательно расположенные на клавиатуре символы («1234», «QWERTY», и т.п.);
- общепринятые сокращения («USER», и т.п.);
- повседневно используемое или распространенное слово (имена или фамилии друзей, коллег, актеров или сказочных персонажей, клички животных);
- что-либо из вышеперечисленного в обратном написании или с добавлением цифр в начале или конце слова.

3.6.4. При смене пароля значение нового пароля должно отличаться от предыдущего не менее чем в 4 позициях.

3.6.5. Для различных информационных систем, сервисов и ресурсов необходимо устанавливать собственные, отличающиеся пароли.

3.7. Рекомендации и примеры по созданию собственного крипоустойчивого пароля приведены в приложении № 1 к Порядку.

3.8. В случае, если данные для авторизации пользователя становятся общедоступными (являются скомпрометированными), либо имеется основание подозревать о возможной компрометации учетных данных, пользователь обязан незамедлительно сообщить о данном факте непосредственному руководителю и в социальную службу по выплате мер социальной поддержки.

3.9. Пользователь несет персональную ответственность в соответствии с законодательством и внутренними нормативными актами Учреждения за свои действия, послужившие причиной компрометации данных для авторизации в информационных системах, сервисах и ресурсах Учреждения.

4. Предоставление (изменение) доступа к информационным системам, сервисам и ресурсам

4.1. Для предоставления доступа пользователю к информационным системам, сервисам и ресурсам Учреждения необходимо выполнение одного из следующих условий:

- доступ необходим для выполнения пользователем должностных обязанностей в соответствии со своей должностной инструкцией (для работников Учреждения);
- доступ необходим для выполнения пользователем обязанностей другого пользователя по указанию (в виде приказа или распоряжения) директора Учреждения (для работников Учреждения);
- доступ необходим для обеспечения информированности пользователя;
- доступ необходим для выполнения пользователем работ в ходе реализации контрактов (договоров), заключенных Учреждением (для работников сторонних организаций).

4.2. Основанием для предоставления/изменения прав доступа к информационным системам, сервисам и ресурсам Учреждения является подписанная соответствующими ответственными лицами Заявка, оформленная по установленной форме (приложение № 2 к Порядку).

4.3. Ответственность за содержание, полноту, достоверность и своевременное представление информации, указанной в Заявке, возлагается на ответственное лицо, подписавшее Заявку.

4.4. Рассмотрение Заявки осуществляется администратором соответствующей информационной системы, сервиса или ресурса, указанным в п. 1.3 настоящего Порядка, в течении двух рабочих дней. Учетные данные для доступа к информационным системам, сервисам и ресурсам (логин и пароль) выдаются пользователю лично, под роспись. Пользователь в обязательном порядке ознакамливается с требованиями по информационной безопасности (приложение № 3 к Порядку). Сведения о выдаче учетной записи пользователя и ознакомлении с требованиями информационной безопасности заносятся в Журнал учета идентификационных данных пользователей информационных систем, сервисов и ресурсов (приложение № 4 к Порядку).

4.5. В случае если доступ к информационной системе, сервису или ресурсу согласно Заявке по какой-либо причине не может быть предоставлен, Заявка возвращается инициатору с подробным описанием данной причины.

5.Аннулирование/блокирование доступа к информационным системам, сервисам и ресурсам

5.1.Аннулирование/блокирование доступа пользователя к ресурсам происходит в случаях:

- изменения должностных обязанностей пользователя;
- длительного обоснованного периода отсутствия (например, декретный отпуск, отпуск по уходу за ребенком);
- нарушения пользователем правил доступа к ресурсу;
- увольнение пользователя;
- по иным распоряжениям директора Учреждения.

Аннулирование/блокирование доступа должно быть инициировано не позднее пяти рабочих дней с момента возникновения соответствующего события.

5.2. Обязанности по инициированию аннулирования/блокирования доступа пользователя к ресурсам возлагаются на руководителя соответствующего структурного подразделения Учреждения.

5.3 Информация об инициировании аннулирования/блокирования доступа (с указанием причины) направляется специалисту по социальной работе социальной службы по выплате мер социальной поддержки соответствующей информационной системы, сервиса или ресурса в произвольной форме в письменном виде за подписью заведующего соответствующего структурного подразделения Учреждения.

5.4.Аннулирование/блокирование доступа осуществляется администратором соответствующей информационной системы, сервиса или ресурса, указанным в п. 1.3. настоящего Положения.

5.5. Сведения об аннулировании/блокировании учетной записи пользователя заносятся в Журнал учета идентификационных данных пользователей информационных систем, сервисов и ресурсов.

Приложение № 1
к Порядку администрирования и предоставления, прав доступа пользователей к информационным системам, сервисам и ресурсам ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»

Рекомендации пользователю по выбору личного пароля

Личный пароль к информационным системам, сервисам и ресурсам Учреждения, отвечающий требованиям криптойстойчивости, можно создать следующими способами:

1) **Сформировать пароль с помощью генератора паролей посредством соответствующих он-лайн сервисов** (например, на ресурсе https://passgenerator.ru);

Он-лайн сервисы при создании паролей позволяют установить требования к нему по длине и используемым символам.

Плюсом такого способа является достаточная надежность и криптоустойчивость пароля.

Недостатком является трудность их запоминания, в том числе, с учетом необходимости использования различных паролей для разных информационных систем. Практика показывает, что в данном случае пользователи в большинстве своем записывают такие пароли на материальные носители, что повышает риски их компрометации.

2) Сформировать пароль самостоятельно по следующему алкгоритму:

- придумать нелогичную смешную фразу, которую легко запомнить. Например, «Усталый студент гладит дорогу»;
- выбрать первые три буквы из каждого слова фразы — «устстугладор»;
- набрать полученную последовательность в английской раскладке клавиатуры — «ecncneukf1jh», это основа будущего пароля;
- выбрать номер (или номера) буквы, которая будет записываться в верхнем регистре и после которой, будет стоять специальный символ или цифра. Например, это будет четвертая буква, а в качестве специального символа выбран «К». Получаем:«ecnC#neukfljh».

Плюсом такого способа является достаточная надежность и криптоустойчивость пароля. Также данный способ позволяет сформировать запоминаемые пароли для разных информационных систем. Даже в случае, если пароль забыт, используемый алгоритм позволяет достаточно легко его вспомнить.

Недостатков у данного способа практически не имеется.

Приложение № 2
к Порядку администрирования и предоставления, прав доступа пользователей к информационным системам, сервисам и ресурсам ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»

Кому:

_____

_____

_____

Ф.И.О.

ЗАЯВКА

на предоставление доступа к информационным сервисам и ресурсам ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»

Прошу предоставить сотруднику:

ФИО сотрудника	
Контактный телефон	

доступ к следующим информационным ресурсам Учреждения:

	Наименование сервиса		Права доступа
1.	1С Предприятие		
2.	Портал федерального казначейства		
3.	Бюджет-WEB		
4.	Плагин		
5	СУФД		
6	Сбис		
7	bus.gov.ru»		
8	ЕИС		
9	bus.gov.ru		
10	WEB Торги-КС		
11	АИС ЭСРН РМ		
12	ЕГИССО		

	Вписать иное		

* *отметить знаком «Х» необходимые сервисы, права Доступа — указать в зависимости от необходимости выполнения работы согласно Должностной инструкции (полный Доступ, общий Доступ ичи какое-либо конкретное направление). Обоснование предоставления доступа**

_____

_____

** *- указывается основание для предоставления соответствующих прав Доступа (например согласно Должностным инструкциям).*

ФИО Руководителя	
Должность	
Контактный телефон	

Дата

_____ Подпись _____/_____/

Бланк для передачи в отдел технической поддержки

В соответствии с заявкой и предоставленным доступом прошу обеспечить техническую возможность подключения АРМ пользователя

_____

к ИС

_____

_____

Специалист по социальной работе социальной службы по выплате мер социальной поддержки _____

Бланк для выдачи сотруднику

Учетная запись сотрудника	Пароль, логин

Учетные данные (логин/пароль) сотрудник получает в отделе информационной безопасности лично под роспись.

Приложение № 3

к Порядку администрирования и предоставления, прав доступа пользователей к информационным системам, сервисам и ресурсам ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»

Лист ознакомления с основными требованиями информационной безопасности при работе с информационными системами, сервисами и ресурсами Учреждения

Я, _____

_____

ознакомлен с основными требованиями информационной безопасности при работе с информационными системами, сервисами и ресурсами Учреждения, а именно уведомлен о том, что пользователь **ОБЯЗАН:**

- использовать и своевременно менять пароли доступа к информационным системам, сервисам и ресурсам в соответствии с периодичностью, установленной внутренними нормативными актами Учреждения;

- в случае подозрения на то, что пароль стал кому-либо известен (скомпрометирован), поменять пароль и сообщить о факте компрометации непосредственному руководителю и в социальную службу по выплате мер социальной поддержки;

- незамедлительно сообщить в социальную службу по выплате мер социальной поддержки в случае получения от кого-либо просьбы сообщить пароль доступа к информационным ресурсам Учреждения;

- при применении внешних носителей информации (например флеш-карт) перед началом работы провести их проверку на предмет наличия компьютерных вирусов средствами антивирусной защиты персонального компьютера.

Пользователю **ЗАПРЕЩАЕТСЯ:**

- передавать или иным способом сообщать другим лицам, в том числе другим сотрудникам Учреждения, личные идентификационные данные (логин/пароль);

- хранить записанные или иным способом размещенные на материальном носителе личные идентификационные данные (логин/пароль) в легкодоступном месте;

- указывать пароль доступа к информационным ресурсам Учреждения в сообщениях электронной почты;

- сохранять логин/пароль в информационной системе Учреждения;

- использовать один и тот же пароль для доступа к различным информационным ресурсам;

- использовать персональный компьютер, периферийное оборудование (принтеры, сканеры и т.п.), а также компоненты программного и аппаратного обеспечения не по назначению (в неслужебных целях);

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств персонального компьютера или устанавливать дополнительно любые программные и аппаратные средства;

- осуществлять обработку конфиденциальной информации, в том числе персональных данных, в присутствии посторонних (не допущенных к данной информации) лиц;

- оставлять включенным без присмотра свой персональный компьютер, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры — комбинации клавиш Win + «L>> или Ctrl + Alt + Delete);

- оставлять без личного присмотра на рабочем месте или где бы то ни было - носители конфиденциальной информации, в том числе содержащие персональные данные;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям информационной безопасности персональных данных.

_____ Дата Подпись

Приложение № 4
к Порядку администрирования и предоставления, прав доступа пользователей к информационным системам, сервисам и ресурсам
ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»

ЖУРНАЛ
учета идентификации данных пользователей информационных систем, сервисов и ресурсов
ГКУ «Соцзащита населения по Инсарскому району РМ (межрайонная)»

№п/п	ФИО сотрудника, должность	Наименование ИС (ИР)	Права доступа	Логин	Роспись в получении ИД, дата	Отметка об аннулировании/блокировании ИД	Примечание

Всего прошнуровано, пронумеровано, скреплено гербовой печатью 6 (Шесть) листов
Директор С.В. Анисимова
Специалист по кадрам М.А.Метликина