# Рекомендации по информационной безопасности

## I. Общие положения

1.1. Настоящий документ определяет общие требования по информационной безопасности к работникам Учреждения при осуществлении трудовой деятельности.

## II. Порядок доступа в Учреждение

2.1. При наличии технической возможности доступ работников на территорию Учреждения должен производиться только с использованием системы контроля и управления доступом Учреждения.

2.2. Каждый работник Учреждения при входе/выходе в Учреждение должен использовать пропуск.

2.3. В случае утери пропуска работники Учреждения незамедлительно уведомляют любым доступным способом непосредственного руководителя.

2.4. Работнику запрещается передавать свой пропуск третьим лицам и другим работникам Учреждения с целью его использования;

2.5. Доступ на территорию Учреждения лиц, не являющихся работниками Учреждения, должен производиться в сопровождении того работника, которому необходимо присутствие гражданина для решения рабочих вопросов

## III. Защита от несанкционированного доступа в помещениях Учреждения

3.1. По окончании рабочего дня, а также в случае одновременного отсутствия всех работников в одном помещении в течении рабочего дня, двери в обязательном порядке должны быть закрыты на ключ.

3.2. В помещениях Учреждения должна быть исключена возможность нахождения лиц, не являющихся работниками Учреждения при отсутствии визуального контроля со стороны работников Учреждения.

## IV. Работа с документами и носителями информации

4.1. Запрещается выносить рабочие документы на бумажных или иных носителях информации (флеш-карты, внешние накопители и др.) за пределы территории Учреждения без служебной необходимости.

4.2. Уничтожение документов на бумажных носителях должно производиться работниками Учреждения только с использованием оборудования Учреждения.

4.3. Запрещается утилизировать рабочие документы в урны для мусора, корзины для макулатуры, предварительно не подвергнув их процедуре уничтожения.

4.4. В случае утери рабочих документов и иных носителей информации (флеш-карты, внешние накопители и др.) необходимо незамедлительно сообщить об этом своему непосредственному руководителю.

4.5. Рекомендуется исключить использование работниками Учреждения иностранных облачных ресурсов для совместного редактирования, таких как «Google Docs».

## V. Работа с автоматизированными рабочими местами Учреждения

5.1. Работникам Учреждения необходимо располагать экран монитора в помещении во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами (шторы на оконных проемах должны быть завешаны, жалюзи закрыты);

5.2. При отсутствии визуального контроля Работника за автоматизированным рабочим местом (далее - АРМ) работникам Учреждения необходимо блокировать доступ. Для блокировки необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка> либо заблокировать доступ иным способом, предусмотренным в операционной системе.

5.3. Работникам Учреждения по окончании рабочего дня необходимо выйти из операционной системы (либо заблокировать АРМ).

5.4. Для предоставления доступа к информационным системам, информационным ресурсам, каналам связи, Работникам Учреждения необходимо отправлять заявку в Службу поддержки пользователей по адресу электронной почты spp@permkrai.ru или по телефону +7 (342) 258 22 44.

5.5. Работникам Учреждения запрещается самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств (за исключением технических специалистов Учреждения).

5.6. Работникам Учреждения запрещается несанкционированно открывать общий доступ к каталогам на АРМ, а также производить удаленное подключение к АРМ по незащищенным каналам связи.

5.7. Работникам Учреждения запрещается подключать к АРМ личные съемные машинные носители информации и мобильные устройства, а также копировать информацию, ставшую им известной в ходе выполнения должностных обязанностей на такие носители без служебной необходимости.

5.8. Работникам Учреждения запрещается отключать (удалять) установленные на АРМ средства защиты информации.

5.9. Работникам Учреждения запрещается привлекать лиц, не являющихся работниками Учреждения, для осуществления установки программного обеспечения, ремонта или настройки технических средств АРМ (за исключением случаев, когда данные услуги оказываются на договорной основе);

5.10. Работникам Учреждения запрещается производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств АРМ (за исключением технических специалистов Учреждения).

5.11. Работникам Учреждения рекомендуется исключить использование личных автоматизированные рабочие места (ноутбуки, компьютеры) для выполнения своих должностных обязанностей.

5.12. Работникам Учреждения запрещается осуществлять фото- и видео съемку рабочих документов, а также публикацию таких документов в социальных сетях и других открытых ресурсах (за исключением случаев, когда это необходимо для выполнения должностных обязанностей).

5.13. Работникам Учреждения запрещается производить деструктивные действия в отношении АРМ Учреждения.

5.14. Работникам Учреждения необходимо соблюдать правила парольной защиты при работе с АРМ (раздел VI настоящего документа).

5.15. Работникам Учреждения необходимо соблюдать правила работы в сети Интернет (раздел VII настоящего документа).

5.16. Работникам Учреждения необходимо соблюдать правила антивирусной защиты (раздел VIII настоящего документа).

5.17. Работникам Учреждения необходимо не допускать случаев социальной инженерии и фишинга (раздел IX настоящего документа).

## VI. Правила парольной защиты

### 6.1. Требования к паролю

6.1.1 Пароль не должен содержать имя учетной записи пользователя или какую-либо его часть;

6.1.2 Пароль должен состоять не менее чем из 6 символов;

6.1.3 В числе символов пароля обязательно должны присутствовать цифры и буквы как в верхнем, так и нижнем регистрах;

6.1.4 Буквенная часть пароля должна содержать как строчные, так и прописные (заглавные) буквы.

6.1.5. Запрещается использовать в качестве пароля простые пароли, такие как «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о работнике.

6.1.6. Пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения;

6.1.7. При смене пароля новое значение должно отличаться от предыдущего не менее чем на четыре символа.

6.1.8. Смена пароля должна производиться не реже одного раза в 90 дней, если иное не предусмотрено нормативной документацией Учреждения.

### 6.2. Правила ввода пароля

6.2.1 Ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан.

6.2.2 Во время ввода пароля необходимо исключить возможность его раскрытия иными лицам, в том числе с помощью технических средств (видеокамеры и др.).

### 6.3. Правила хранения пароля

6.3.1 Рекомендуется не записывать пароль на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

6.3.2 Запрещается сообщать другим работникам и третьим лицам личный пароль от АРМ;

6.3.3 Работникам Учреждения необходимо своевременно сообщать непосредственному руководителю об утере, компрометации, несанкционированном изменении паролей.

## VII. Правила работы в сети Интернет

### 7.1. При работе в сети Интернет работник Учреждения обязан:

7.1.1 Производить работу в сети Интернет исключительно в целях исполнения своих должностных обязанностей;

7.1.2 Противодействовать методам социальной инженерии: не открывать вложения в письмах от неизвестных источников, не переходить по подозрительным баннерам и ссылкам на веб-сайтах, проверять вводимый адрес веб-сайтов на предмет опечаток.

7.1.3 Обращаться к непосредственному руководителю в случае выявления фактов нарушения информационной безопасности.

**7.2 При работе в сети интернет работнику Учреждения запрещается:**

7.2.1 Посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, торрент-сайты, и т.д.) и скачивать с таких сайтов какие-либо файлы и программное обеспечение.

7.2.2 Нецелевое использование подключения к сети «Интернет» (просмотр фильмов, скачивание игр и т.д.).

**7.3 Использование электронной почты**

7.3.1 Каждому работнику Учреждения при трудоустройстве должен создаваться служебный адрес электронной почты, размещенный на почтовом сервере Единого почтового домена Пермского края, в адресном пространстве permkrai.ru;

7.3.2. При увольнении работника Учреждения служебный адрес электронной почты в обязательном порядке подлежит удалению;

7.3.3. Не допускается передача учетных данных (логин, пароль) электронной почты другим работникам Учреждения и третьим лицам;

7.3.4. Использовать в служебных целях личные адреса электронной почты запрещается;

7.3.5. Не допускается использование электронной почты для отправки информации содержащей персональные данные;

7.3.6. Не допускается использование электронной почты для отправки конфиденциальной информации, информации ограниченного доступа и информации, содержащей государственную тайну;

7.3.7. Для приема обращений граждан не допустимо использование сторонних почтовых сервисов не отвечающих требованиям безопасности в соответствии с действующим законодательством в области защиты персональных данных;

7.3.8. Для направления ответов на обращения граждан рекомендуется использовать только служебный адрес электронной почты, размещенный на почтовом сервере Единого почтового домена Пермского края, в адресном пространстве permkrai.ru.

**7.4. Использование социальных сетей в рабочих целях**

7.4 В случае, если должностными обязанностями работника предусмотрено использование социальных сетей («Вконтакте», «Instagram», и др.) (Далее - Приложение) необходимо:

7.4.1 Ознакомиться с политикой использования Приложения;

7.4.2 Не загружать конфиденциальную информаций в Приложение (В т.ч. Персональные данные);

7.4.3 Исключить передачу учетных данных (логин, пароль) третьим лицам и другим работникам Учреждения;

7.4.2 В случае наличия технической возможности Приложения использовать двухфакторную аутентификацию.

## VIII. Соблюдение антивирусной защиты информации

**8.1. Работник Учреждения обязан:**

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник обязан самостоятельно или совместно с непосредственным руководителем и/или техническим специалистом Учреждения провести внеочередной антивирусный контроль АРМ;

8.1.2 Производить антивирусную проверку отчуждаемых машинных носителей (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

8.1.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов:

- приостановить работу с АРМ;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов непосредственным руководителем и/или техническим специалистом Учреждения;

8.1.4 периодически, не реже одного раза в неделю, проводить проверку антивирусом на наличие вирусного заражения (в случаях, если проверка не производится автоматически)

**8.2. Работнику Учреждения запрещается:**

8.2.1 Удалять средства антивирусной защиты, установленные на АРМ;

8.2.2. Вносить изменения в настройки средства антивирусной защиты, установленного на АРМ.

## IX. Противодействие социальной инженерии и фишингу

9.1. Социальная инженерия – совокупность приемов и методов, применяемых злоумышленниками, направленных на получение от работника служебной (конфиденциальной) информации;

9.1.1. В целях противодействия социальной инженерии работникам Учреждения необходимо:

- не сообщать по электронной почте и по телефону служебной информации пока не будет установлена личность запрашивающего и его право на доступ к такой информации;
- не осуществлять работу за АРМ и с документами в присутствии посторонних лиц;
- блокировать АРМ (при отсутствии за рабочим местом, при окончании рабочего дня и т.д.);
- в случае попытки посторонних лиц получить от работника служебную (конфиденциальную) информацию, незамедлительно сообщить об этом непосредственному руководителю;

9.2. Фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам, паролям и т.д.).

9.2.1. В целях противодействия фишингу работникам Учреждения необходимо:

- осуществлять проверку адреса любого сайта, который запрашивает идентификационную информацию;
- осуществлять проверку электронной почты отправителя писем;
- не проходить по подозрительным ссылкам и не скачивать подозрительные файлы.
- об утере или компрометации логинов и паролей сообщать ответственному работнику отдела информационной безопасности Учреждения.

## X. Проведение совещаний в формате Видеоконференции

10.3 Рекомендуется исключить использование работниками Учреждения в служебных целях иностранных сервисов для проведения видеоконференций (Zoom, Skype, и др.) в ходе исполнения должностных обязанностей.

## XI. Использование облачных ресурсов для хранения информации в служебных целях

11.1 Рекомендуется исключить использование облачных ресурсов для хранения информации, таких как «Google Диск», «Яндекс.Диск» и иных облачных ресурсов.

## XII. Удаленная (дистанционная) работа

12.1 При установлении удаленного (дистанционного) режима работы правила настоящей инструкции должны соблюдаться в полном объеме.

## XIII. Обработка персональных данных

13.1. Обработка персональных данных работниками Учреждения должна производиться с соблюдением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

## XIV. Подготовка технических заданий и проведение закупочных процедур

14.1. Запрещается привлекать к подготовке технических заданий лиц, не являющихся работниками Учреждения.

14.2. Запрещается разглашать сведения об осуществлении закупок товаров, работ, услуг для обеспечения государственных нужд в соответствии с Федеральным законом от 05.04.2013 г. N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» до момента их официального опубликования, а именно, извещения, технические задания и иную информацию, относящуюся к процедурам определения поставщика (конкурсную, аукционную документацию и т.д.).

## XV. Соблюдение конфиденциальности

15.1. Разглашение работниками Учреждения конфиденциальной информации, закрепленной в локальных нормативно-правовых актах Учреждения, третьим лицам не допускается.

## XVI. Ответственность работника за нарушение правил информационной безопасности

16.1. Ответственность за нарушение правил информационной безопасности несет каждый работник Учреждения в пределах своих служебных обязанностей и полномочий.

16.2. На основании ст. 192 Трудового кодекса Российской Федерации работники, нарушающие правила настоящего документа, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

16.3. На основании ст. 238 Трудового кодекса РФ все работники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Учреждению в результате нарушения ими правил настоящего документа.

16.4 На основании ст. 81 Трудового кодекса Российской Федерации с работником может быть расторгнут трудовой договор, в случае разглашения Работником охраняемой законом тайны (коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника.