УТВЕРЖДАЮ
Председатель администрации
Тес-Хемского кожууна
_____ / Т.С. Самдан /
«17» февраля 2021 г.

ИНСТРУКЦИЯ
пользователя по обеспечению правил информационной безопасности при работе в информационных системах персональных данных

1. Общие положения

1.1. Пользователем персональных данных (далее – Пользователь) является муниципальный служащий (работник) Администрации Тес-Хемского кожууна Республики Тыва, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных (далее – ПДн).

1.2. Пользователь несет персональную ответственность за свои действия.

1.3. Методическое руководство работой пользователя осуществляется ответственным за организацию обработки персональных данных (далее – Ответственный).

2. Обязанности Пользователя

2.1. Знать и выполнять требования действующих нормативных методических документов, а также внутренних организационно-распорядительных документов, регламентирующих порядок обработки и защиты ПДн при их обработке.

2.2. Выполнять указания Ответственного и Администратора безопасности информационной системы персональных данных.

2.3. Соблюдать режим допуска в помещения, где проводится обработка ПДн.

2.4. Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него должностными обязанностями и на основании Разрешительной системы допуска пользователей к информационным системам персональных данных.

2.5. Знать и строго выполнять правила работы со средствами защиты информации, установленными на элементах информационной системы персональных данных (далее – ИСПДн).

2.6. Хранить втайне от других свой пароль.

2.7. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.8. Использовать при работе только учтённые машинные носители информации.

2.9. Перед началом работы с машинными носителями информации осуществить проверку носителя на предмет отсутствия компьютерных вирусов.

2.10. Передавать для хранения установленным порядком свое устройство личной идентификации, личную ключевую дискету и другие реквизиты разграничения доступа (при необходимости их использования) только Ответственному.

2.11. При выводе ПДн на бумажный носитель (печать) необходимо фиксировать распечатанный документ в журнале учета подготовленных документов (исходящих, внутренних).

2.12. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций необходимо обратиться к Администратору безопасности информационной системы персональных данных.

2.13. Пользователям запрещается:

- разглашать сведения, содержащие ПДн, третьим лицам;
- обрабатывать на автоматизированных рабочих местах информацию и выполнять другие работы, не предусмотренные Разрешительной системой доступа к ресурсам, программным, и техническим средствам соответствующей информационной системы персональных данных;
- фиксировать на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;
- записывать и хранить информацию на незарегистрированных машинных носителях информации;
- подключать к рабочей станции незарегистрированные машинные носители информации;
- подключать к рабочей станции личные машинные носители информации и мобильные устройства;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение,
- изменять установленный алгоритм функционирования технических и программных средств, вскрывать и ремонтировать технические средства;
- открывать общий доступ к папкам на своей рабочей станции;

- отключать (блокировать) средства защиты информации; - сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

- привлекать посторонних лиц для производства ремонта или настройки автоматизированных рабочих мест без согласования с Ответственным;

- оставлять посторонних лиц без присмотра в помещениях, где ведется обработка ПДн;

- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

- передавать ПДн по открытым каналам связи.

2.14. Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью уменьшения либо ликвидации их последствий.

2.15. 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] или [Windows] [L].

2.16. Обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

2.17. При покидании помещения, где ведется обработка персональных данных, необходимо запирать данные помещения на ключ.

3. Порядок реагирования на аварийную ситуацию

3.1. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных ниже:

- отключение электроэнергии;

- сбой в работе вычислительной сети (коммутационного оборудования);

- ошибка персонала, имеющего доступ к серверной;

- нарушение конфиденциальности, целостности и доступности персональных данных;

- физический разрыв внешних каналов связи.

3.2. В случае реализации любой из угроз (выявлении предпосылок к ее реализации) Пользователь обязан:

- предпринять попытку сохранения обрабатываемой информации, содержащей ПДн;

- прекратить работу на автоматизированном рабочем месте;

- немедленно оповестить Ответственного, Администратора безопасности информационной системы персональных данных, о возникновении аварийной ситуации.