**Администрация Верхнекетского района**

**РАСПОРЯЖЕНИЕ**

|  |  |  |
| --- | --- | --- |
|  3 марта 2023 г. | р.п. Белый ЯрВерхнекетского района Томской области | № 21-р |

**О** **назначении лиц, ответственных за прекращение доступа**

**работников к персональным данным, обрабатываемым в Администрации Верхнекетского района**

Для обеспечения защиты персональных данных (ИСПДн), обрабатываемых в Администрации Верхнекетского района,

1. Обязать главного специалиста по общим вопросам управления делами (Хмылеву Н.Г.) извещать Администратора безопасности о следующих ситуациях:

– об увольнении работника Администрации Верхнекетского района, в обязанности которого входит работа с персональными данными (ПДн);

– об изменении должности или должностной инструкции работника Администрации Верхнекетского района, влекущем за собой потерю необходимости доступа к ПДн.

1. Ответственный работник обязан известить Администратора безопасности не позднее чем через день после подписания соответствующих документов об увольнении работника или изменении его должности или должностной инструкции.
2. Администратор безопасности после получения указанной выше информации обязан не позднее чем через день принять меры по прекращению доступа работника к ИСПДн и ПДн, а так же в помещения, где производится работа с ИСПДн и ПДн.
3. Инструкция Администратора безопасности по прекращению доступа работника к ПДн представлена в Приложении №1 к настоящему приказу.
4. Признать утратившим силу распоряжение Администрации Верхнекетского района от 16 марта 2018 года №31-р «О назначении лиц, ответственных за прекращение доступа работников к персональным данным, обрабатываемым в Администрации Верхнекетского района .
5. Контроль за исполнением настоящего распоряжения возложить на начальника отдела информационных технологий Засухина В.И..

Глава Верхнекетского района С.А. Альсевич

Генералова Т.Л.

|  |  |
| --- | --- |
| С распоряжением ознакомлен |  |

Дело-1, управление делами-1, ОИТ-1.

Приложение №1 к распоряжению Администрации Верхнекетского района от «03» марта 2023 года №21-р

Инструкция Администратора безопасности по прекращению доступа работника к персональным данным

1. Администратор безопасности обязан прекратить доступ работника к персональным данным (далее – ПДн), обрабатываемым в Администрации Верхнекетского района, в следующих случаях:

– увольнение работника, имеющего доступ к ПДн в рамках своих обязанностей;

– изменение должности или изменение должностной инструкции работника, что влечет за собой потерю необходимости доступа к ПДн;

– появление подозрений у службы безопасности или Администратора безопасности о том, что работник может производить действия, влекущие за собой утечку ПДн, обрабатываемых в Администрации Верхнекетского района.

1. Главная задача Администратора безопасности после получения информации о какой-либо из ситуаций, указанных в п.1 приказа – ограничить доступ сотрудника к информационным системам персональных данных (далее – ИСПДн) и в кабинеты, где производится работа с ИСПДн и ПДн.
2. Порядок действий Администратора безопасности:
3. Получить полный список информационных систем и помещений, в которые имеет доступ работник;
4. Если работник имеет доступ в некоторую ИСПДн с помощью личной учетной записи – необходимо удалить или заблокировать данную учетную запись;
5. Если работник имеет доступ в некоторую ИСПДн с помощью общей учетной записи (учетная запись, которой пользуются двое или более работников) – необходимо сменить пароль данной учетной записи, известив остальных работников о новом пароле и о запрете передавать новый пароль работнику, исключенному из числа пользователей учетной записи;
6. Если работнику для выполнения должностных обязанностей были выданы съемные носители или ключевые носители, используемые в работе с ИСПДн – данные носители должны быть изъяты, с занесением информации об изъятии в соответствующие журналы и подписью Ответственного лица. При этом для каждого ключевого носителя необходимо сменить пароль, используемый для доступа к содержимому ключевого носителя, а при подозрении на компрометацию содержимого – сменить содержимое ключевого носителя (сертификаты электронной подписи и т.п.);
7. Если работник имеет доступ в одно или несколько помещений, где производится работа с ПДн – необходимо внести изменения в локальные акты, регламентирующие доступ работников в данные помещения, о запрете доступа указанному работнику в эти помещения без сопровождения ответственных лиц, а так же изъять ключи и идентификаторы, необходимые для доступа в них; при этом о данном запрете необходимо сообщить ответственным лицам этих помещений и службе охраны;
8. Если работнику были выданы какие-либо документы, содержащие ПДн или иную информацию, определенную как «конфиденциальная» в соответствии с документом «Перечень сведений конфиденциального характера в Администрации Верхнекетского района, или он был назначен ответственным за какие-либо документы конфиденциального характера – необходимо проконтролировать возврат всех документов. Также необходимо назначить ответственным за данные документы другого работника в Администрации Верхнекетского района. Ответственность за полноту возврата документов лежит на начальнике отдела информационных технологий.