

**Порядок
доступа работников Администрации в помещения, в которых ведется обработка
персональных данных**

1. Настоящий Порядок доступа муниципальных служащих и работников Администрации (далее - Работники) в помещения, в которых ведется обработка персональных данных, (далее - Порядок) устанавливает единые требования к доступу Работников Администрации в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в администрации, и обеспечения соблюдения требований законодательства о персональных данных.

2. Настоящий Порядок обязателен для применения и исполнения всеми Работниками администрации.

3. Помещения, в которых ведется обработка персональных данных, должны отвечать определенным нормам и исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в этих помещениях документов и средств автоматизации.

4. Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время.

5. По завершению рабочего дня, помещения, в которых ведется обработка персональных данных, закрываются.

6. Вскрытие помещений, где ведется обработка персональных данных, производят Работники, работающие в этих помещениях.

7. При отсутствии сотрудников администрации, работающих в этих помещениях, помещения могут быть вскрыты комиссией, созданной по указанию главы Администрации.

8. В случае утраты ключей от помещений немедленно заменяется замок.

9. Уборка в помещениях, где ведется обработка персональных данных, производится только в присутствии служащих, работающих в этих помещениях.

10. При обнаружении повреждений запоров или других признаков, указывающих на возможное проникновение в помещения, в которых ведется обработка персональных данных, посторонних лиц, эти помещения не вскрываются, а составляется акт и о случившемся немедленно ставятся в известность глава Администрации и органы МВД.

11. Одновременно принимаются меры по охране места происшествия и до прибытия работников органов МВД в эти помещения никто не допускается.

ПЕРЕЧЕНЬ
информационных систем персональных данных в Администрации

1. Программа «СУФД»
2. ГАС «Управление»
3. Росреестр.
4. ГИС ЖКХ
5. ФИАС
6. ФГИС ТП.
7. ЕИС в сфере закупок.
8. ЕПБС.
9. WEB – консолидация.
10. WEB – планирование.
11. WEB – исполнение.

Журнал
учета съемных носителей персональных данных

Начат: [число, месяц, год]
Окончен: [число, месяц, год]
На ___ листах

Ответственный за хранение [должность, Ф.И.О., подпись]

N п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Причина и основание окончания использования
1	2	3	4	5	6	7
						[номер и дата отправки адресату или распоряжения о передаче, номер и дата акта утраты, неисправность, заполнение подлежащими хранению данными]

**Журнал
учета событий информационной безопасности**

Журнал начат « » 20 г.	Журнал завершен « » 20 г.
Должность /	Должность /
/	/

N п/п	Дата события	Основания возникновения события	Описание события (мероприятия)	Характеристика события	(ФИО, субъекта)	Должность, ФИО и подпись ответственного за ведение журнала	Примечание