Правила организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения в

МБОУ СОШ с.Тербуны

1. Настоящие правила устанавливают требования к организации режима обеспечения безопасности помещений МБОУ СОШ с.Тербуны (далее - Организация), в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.
2. Пропускной режим предусматривает:

* защиту от проникновения посторонних лиц в помещения Организации, которая обеспечивается организацией режима доступа.
* запрет на внос и вынос за пределы помещения материальных носителей персональных данных;
* определение перечня должностных лиц, имеющих право доступа в помещение.

3. Внутриобъектовый режим предусматривает:

* назначение ответственного за помещения;
* помещения, в которых обрабатываются персональные данные с использованием средств автоматизации и без использования таких средств, должны иметь прочные двери, оборудованные механическими замками, а при необходимости, замками с контролем доступа;
* в нерабочее время помещение должно закрываться;
* в случае ухода в рабочее время из помещений работников, необходимо эти помещения закрыть на ключ;
* уборка помещений должна производиться в присутствии лица, ответственного за эти помещения.
* пребывание в помещениях посторонних лиц, не имеющих права доступа в эти помещения, разрешено только после согласования с директором Организации или лицом, ответственным за организацию обработки персональных данных, и в сопровождении лица, работающего в этих помещениях.
* контроль за пребыванием в помещениях посторонних лиц, не имеющих права доступа в эти помещения, осуществляет ответственный за это помещение.

4. Защита информационной системы и машинных носителей персональных  
данных от несанкционированного доступа, повреждения или хищения

1. В период эксплуатации информационных систем персональных данных должны быть предусмотрены меры по исключению случаев несанкционированного доступа при проведении ремонтных, профилактических и других видов работ.
2. В случае необходимости проведения ремонтных работ средств вычислительной техники, входящих в состав информационной системы, с привлечением специализированных ремонтных организаций обеспечивается обязательное гарантированное уничтожение (стирание) персональных данных и другой конфиденциальной информации, записанной на материальном носителе, под контролем лица, ответственного за организацию обработки персональных данных с составлением соответствующего акта.

4.3. Хранение съемных машинных носителей персональных данных должно исключать возможность несанкционированного доступа к ним.

5. Работники Организации должны ознакомиться с настоящими Правилами под подпись.

|  |  |  |  |
| --- | --- | --- | --- |
| Лист ознакомлений с порядком доступа сотрудников в помещения,  в котором ведется обработка персональных данных | | | |
| №  п/п | Ф.И.О. | Дата  ознакомления | Подпись |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| 5. |  |  |  |
| 6. |  |  |  |
| 7. |  |  |  |
| 8. |  |  |  |
| 9. |  |  |  |
| 10. |  |  |  |
| 11. |  |  |  |
| 12. |  |  |  |
| 13. |  |  |  |
| 14. |  |  |  |
| 15. |  |  |  |
|  | И т.д. |  |  |
|  |  |  |  |
|  |  |  |  |

**Лист ознакомлений**

**с правилами организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этом помещении лиц, не имеющих права доступа в эти помещения**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Фамилия, имя, отчество | Наименование  подразделения,  отдела | Дата  ознакомления | Подпись |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |