УТВЕРЖДАЮ:
Заведующий детским садом №62 ОАО «РЖД»
_____ С.В.Романова
приказу от 11.01.2021 г.№40

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.

1. Настоящие правила устанавливают требования к организации режима обеспечения безопасности помещений детского сада №62 ОАО «РЖД» (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 быть закрыто;
   - в случае ухода в рабочее время из помещения 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 заведующим 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.
   - В период эксплуатации информационных систем персональных данных должны быть предусмотрены меры по исключению случаев несанкционированного доступа при проведении ремонтных работ, профилактических и других видов работ.
   - 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.

- Хранение съёмных машинных носителей персональных данных должно исключать возможность несанкционированного доступа к ним.

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