СОГЛАСОВАНО

Председатель ППО
РЖД детского сада № 26
_____ О.А. Лазарева
Протокол № 63-1 от 09.01.2025 г.

УТВЕРЖДАЮ

Заведующий
РЖД детским садом № 26
_____ Е.В. Епифанцева
Приказ № 38.3/А от 09.01.2025 г.

П О Л И Т И К А
по работе с инцидентами информационной безопасности на 2025 г.

Настоящая политика разработана в целях выявления, предотвращения и устранения последствий нарушений законодательства Российской Федерации в области обработки персональных данных в соответствии со ст. 18.1 Федерального Закона № 152-ФЗ «О персональных данных».

1. Общие положения

Политика по работе с инцидентами информационной безопасности (далее – Политика) разработана в соответствии с Федеральным Законом № 152-ФЗ «О персональных данных», Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Инциденты в области информационной безопасности возникают при нарушении правил и требований информационной безопасности.

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов информационных систем персональных данных.

2. Работа с инцидентами включает в себя 3 направления:

- выявление инцидентов в области информационной безопасности;
- реакция на инциденты в области информационной безопасности;
- предупреждение инцидентов в области информационной безопасности.

3. Выявление инцидентов в области информационной безопасности

Работа по выявлению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

- выявление инцидентов в области информационной безопасности с помощью технических средств;

- выявление инцидентов в области информационной безопасности в ходе мероприятий по контролю за обработкой персональных данных.

4. Реакция на инциденты в области информационной безопасности

Реакция на инциденты в области информационной безопасности включает в себя:

- фиксацию инцидента в области информационной безопасности;
- определение границ инцидента и ущерба (в том числе потенциального) от реализации угроз информационной безопасности в ходе инцидента;
- ликвидация последствий инцидента и полное либо частичное возмещение ущерба;
- наказание виновных в инциденте информационной безопасности.

5.Предупреждение инцидентов в области информационной безопасности

Предупреждение инцидентов строится на:

- планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками РЖД детский сад № 26;
- доведении до сотрудников норм законодательства в области защиты персональных данных и внутренних документов, устанавливающих ответственность за нарушение требований информационной безопасности;
- разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимающимися на работу;
- своевременной модернизации системы обеспечения информационной безопасности информационных систем персональных данных с учетом возникновения новых угроз информационной безопасности;
- своевременном обновлении программного обеспечения, в т.ч. баз сигнатур антивирусных средств.