|  |  |
| --- | --- |
| ПРИНЯТО  Общим собранием работников  протокол № \_\_\_\_\_  от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2022 г. | УТВЕРЖДАЮ  Заведующий Детским садом № 261  ОАО «РЖД»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В. В. Лескова  от «\_\_\_\_\_» \_\_\_\_\_\_\_ 2022 г. |
| УЧТЕНО  Мнение Совета родителей  протокол № \_\_\_\_\_  от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2022 г. |  |

**ПОЛИТИКА**

**по работе с инцидентами информационной безопасности**

**Детского сада № 261 ОАО «РЖД»**

1. **Общие положения**

Настоящая политика разработана в целях организации работы с инцидентами информационной безопасности в Детском саду № 261 ОАО «РЖД».

Политика по работе с инцидентами информационной безопасности (далее – Политика) разработана в соответствии с Федеральным Законом N 152-ФЗ «О персональных данных», Федеральным законом N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ N 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

Инцидент – одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее – ИС) и (или) к возникновению угроз безопасности, в том числе персональных данных.

В ходе инцидента реализуются (или создается возможность для реализации) угрозы информационной безопасности, что, как правило, приводит к нанесению вреда активам Детского сада № 261 ОАО «РЖД» и (или) субъекту персональных данных.

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.

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.

# Определение лиц, ответственных за выявление инцидентов и реагирование на них:

# Ответственными за выявление инцидентов в ИС являются:

* лица, имеющие право доступа в ИС;
* ответственные за техническое обслуживание ИС;

**Ответственными за реагирование на инциденты в ИС являются:**

* лица, имеющие право доступа в ИС;
* ответственные за техническое обслуживание ИС;
* заведующий;
* ответственный за обработку персональных данных;
* председатель комиссии по работе с инцидентами.

# 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;
* выявление инцидентов с помощью персонала ЧДОУ.

# 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.

# Предупреждение инцидентов в области информационной безопасности

Предупреждение инцидентов строится на:

* планомерной деятельности по повышению уровня осознания информационной безопасности руководством и работниками;
* проведения мероприятий по обучению работников правилам и способам работы со средствами защиты информационных систем персональных данных;
* доведении до сотрудников норм законодательства в области защиты персональных данных и локальных актов ЧДОУ, 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 антивирусных средств.

1. **Причины инцидентов в области информационной безопасности**

Причинами инцидентов в области информационной безопасности являются:

* действие враждебных интересам ЧДОУ организаций и отдельных лиц;
* отсутствие персональной ответственности за обеспечение информационной безопасности персональных данных работников и руководителя;
* недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности персональных данных;
* отсутствие моральной и материальной стимуляции за соблюдение правил и требований информационной безопасности;
* недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;
* совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;
* наличие привилегированных бесконтрольных пользователей в информационной системе;
* пренебрежение правилами и требованиями информационной безопасности работниками ЧДОУ;
* и другие причины.

**6. Расследование инцидентов в области информационной безопасности**

Расследование инцидентов в области информационной безопасности должно включать в себя:

* формирование комиссии по расследованию инцидента в области информационной безопасности;
* определение границ инцидента – информационных ресурсов, технических средств и персонала, затронутых инцидентом;
* определение причин инцидента, факторов, влияющих на возникновение инцидента;
* определение участников инцидента;
* определение последствий инцидента;
* составление заключения по результатам расследования;
* выработка рекомендаций по предотвращению возникновения подобных инцидентов в будущем.