Обсуждено на Педагогическом совете
Протокол №4 от 30.05.2024 г

Мнение Родительского комитета учтено
Протокол №3 от 30.05.2024

Введено в действие/утверждено
заведующий МАДОУ детский сад № 1 «Страна Детства» Н.В.Булашова
Приказ от 06 июня 2024 г. № 137-ОД

ПОЛОЖЕНИЕ
об информационной безопасности муниципального автономного дошкольного образовательного учреждения детский сад №1 «Страна Детства»

1. Общие положения

1.1. Данное положение об информационной безопасности (далее – положение) разработано в соответствии с Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.). Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации". Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" для Муниципального автономного дошкольного образовательного учреждения детский сад № 1 «Страна Дества» (далее – Детский сад).

1.2. Информационная безопасность является одним из составных элементов комплексной безопасности

1.3. Под информационной безопасностью следует понимать состояние защищенности информационных ресурсов Детского сада, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.4. К объектам информационной безопасности в Детском саду относятся:

- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера:
- информацию, защита которой предусмотрена законодательными актами РФ. в том числе персональные данные:
- средства и системы информатизации. программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

1.5. Система информационной безопасности (далее - СИБ) должна обязательно обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата):
- целостность (точность и полноту информации и компьютерных программ);
- доступность (возможность получения пользователями информации в пределах их компетенции).

1.6 Обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2. Правовые нормы обеспечения информационной безопасности

2.1. Детский сад имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников школы, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз. Детский сад обязан обеспечить сохранность конфиденциальной информации.

2.2. Администрация Детского сада:
- назначает ответственного за обеспечение информационной безопасности;
- издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
- имеет право включать требования по защите информации в договоры по всем видам деятельности;
- разрабатывает перечень сведений конфиденциального характера; - имеет право требовать защиты интересов Детского сада со стороны государственных и судебных инстанций.

2.3. Организационные и функциональные документы по обеспечению информационной безопасности:
- приказ заведующего Детского сада о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных; -
инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников школы и др.

2.4 Порядок допуска сотрудников Детского сада к информации предусматривает:
- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и школы об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. Мероприятия по обеспечению информационной безопасности

3.1. Для обеспечения информационной безопасности в Детском саду требуется проведение следующих первоочередных мероприятий:
- защита интеллектуальной собственности Детского сада;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета;
- организация защиты конфиденциальной информации, в том числе персональных данных работников и обучающихся;
- учет всех носителей конфиденциальной информации.

4. Организационная работа с информационными ресурсами и технологиями

4.1. Система организации делопроизводства:
- учет всей документации Детского сада, в том числе и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов школы в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

4.2. В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:
4.2.1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.
4.2.2. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.
4.2.3. Выданные для работы дела и документы с грифом "Для служебного пользования" ("Ограниченного пользования") подлежат возврату в свой кабинет в тот же день.
4.2.4. Передача документов исполнителю производится только через ответственного за организацию делопроизводства.
4.2.5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы Детского сада.
4.2.6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

4.3.Для организации делопроизводства приказом заведующего Детского сада назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной руководителем. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

5. Обеспечение безопасности на официальном сайте детского сада

5.1. Официальный сайт Детского сада относится к группе многопользовательских информационных систем с разными правами доступа. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных. Официальный сайт Детского сада обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения. Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой на Официальном сайте Детского сада.

5.2. Регламент общих ограничений для участников образовательного процесса при работе со Официальным сайтом, обеспечивающей предоставление Услуги.
5.2.1.Участники образовательного процесса, имеющие доступ к Официальному сайту, не имеют права передавать персональные логины и пароли для входа на Официальный сайт другим лицам. Передача персонального логина и пароля для входа на Официальный сайт другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.
5.2.2. Участники образовательного процесса, имеющие доступ на Официальный сайт, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).
5.2.3. При проведении работ по обеспечению безопасности информации на Официальном сайте, участники образовательного процесса, имеющие доступ к Официальному сайту, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных