МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ " ДЕТСКИЙ САД № 214 КИРОВСКОГО РАЙОНА ВОЛГОГРАДА"

Подписан: МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ДЕТСКИЙ САД № 214 КИРОВСКОГО РАЙОНА ВОЛГОГРАДА"
DN: C=RU, S=Волгоградская область, STREET=ул. им. генерала Шумилова 25а, L=Волгоград, T=заведующий, O="МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ДЕТСКИЙ САД № 214 КИРОВСКОГО РАЙОНА ВОЛГОГРАДА"", OГРН=1023404291701, ОКПО=48084236, СНИЛС=01425631205, ИНН ЮЛ=3447058475, ИНН=344705847577, E=dou214@volgadmin.ru, G=Светлана Викторовна, SN=Борисенкова, CN="МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ДЕТСКИЙ САД № 214 КИРОВСКОГО РАЙОНА ВОЛГОГРАДА""
Основание: Я являюсь автором данного документа
Местоположение: место подписания
Дата: 2021-02-08 14:09:31

МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ДЕТСКИЙ САД № 214 КИРОВСКОГО РАЙОНА ВОЛГОГРАДА»
400011, г. Волгоград, ул. генерала Шумилова, 25а, тел.(факс): (8442) 45-05-84, dou214@volgadmin.ru,
ОКПО 48084236 ОГРН 1023404291701 ИНН 3447014538 КПП 344701001 ОКОПФ20903

СОГЛАСОВАНО
Председатель профкома
_____ Н.В.Игольникова
протокол № 2 от «27» января 2021г.

УТВЕРЖДЕНО:
Заведующий МОУ детский сад № 214
_____ С.В.Борисенкова
Приказ № 38 от 01.02.2021г.

ДОЛЖНОСТНАЯИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ И ВНЕДРЕНИЕ СИСТЕМЫ КОНТЕНТНОЙ ФИЛЬТРАЦИИ В МУНИЦИПАЛЬНОГО ДОШКОЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ «ДЕТСКИЙ САД №214 КИРОВСКОГО РАЙОНА ВОЛГОГРАДА»

1. Общие положения

Настоящий документ определяет основные обязанности, права и ответственность лица за информационную безопасность муниципального дошкольного образовательного учреждения «Детский сад №214 Кировского района Волгограда» (далее - Учреждение)

Ответственный за информационную безопасность назначается приказом руководителя Учреждения.

Ответственный за информационную безопасность осуществляет свою деятельность в интересах Учреждения в информационной сфере путем обеспечения защиты информации и поддержания достигнутого уровня защиты автоматизированных информационных систем (АИС) и ее ресурсов на всех этапах создания, модернизации и эксплуатации АИС.

Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности Учреждения. Защита информации представляет собой комплекс организационных и технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний в отношении технических и программных средств Учреждения и информации, циркулирующей в них.

Ответственный за информационную безопасность несет ответственность за реализацию принятой в Учреждение политики безопасности, закрепленной в Концепции информационной безопасности Учреждения.

Инструкция регулирует отношения между ответственным за информационную безопасность, пользователями АИС, сторонними организациями, возникающие при:

- Эксплуатации развитии АИС;
- формировании и использовании данных, сообщений, баз данных, информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления пользователю документированной информации;
- при создании, внедрении и эксплуатации новых информационных технологий.

Ответственный за информационную безопасность обладает правами доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты.

Требования ответственного за информационную безопасность, связанные с выполнением ими своих функций, обязательны для исполнения всеми пользователями АИС.

2. Обязанности ответственный за информационную безопасность

Ответственный информационную безопасность обязан:

Обеспечить информационную безопасность, защиту конфиденциальной информации, в том числе и на бумажных носителях, от несанкционированного доступа, искажения и уничтожения при ее передаче, обработке и хранении с использованием средств вычислительной техники.

Организовывать доступ пользователей в помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации.

Организовывать, в установленном порядке, передачу информации, составляющей коммерческую тайну Учреждения на сменных магнитных носителях и иными способами.

Организовывать сопровождение работ по категорированию объектов средств вычислительной техники Учреждения.

Знать перечень установленных в подразделениях Учреждения серверов, рабочих станций, средств копировально-множительной техники, устройств и топологию локально вычислительной сети.

Иметь перечень информационных ресурсов Учреждения.

Обеспечить доступ к защищаемой информации пользователям АИС согласно их прав доступа при получении оформленного соответствующим образом разрешения;

Осуществлять оперативный контроль за работой пользователей защищаемых рабочих станций, анализировать содержимое системных журналов всех РС и реагировать на возникающие нештатные ситуации.

Запрещать и немедленно блокировать применение пользователям сети программ, с помощью которых возможны факты несанкционированного доступа к ресурсам АИС.

Не допускать установку, использование, хранение и размножение в АИС программных средств, не связанных с выполнением функциональных задач.

Не допускать к работе на рабочих станциях и серверах ЛВС посторонних лиц.

Аппаратными и программными средствами выявлять факты несанкционированного доступа к информационным ресурсам АИС, а также другие нарушения, которые могут привести к разглашению или утрате конфиденциальной информации, и принимать меры по их пресечению.

Контролировать физическую сохранность средств и оборудования АИС.

Присутствовать при внесении изменений в конфигурацию(модификации) аппаратно программных средств защищенных рабочих станций и серверов.

Участвовать в приемке новых программных и аппаратных средств;

Периодически проверять состояние используемых СЗИНС'Д. осуществлять проверку правильности их настройки.

Периодически контролировать целостность печатей(пломб, наклеек) на устройствах защищенных рабочих станций

Вести контроль за процессом резервирования и дублирования важных ресурсов АИС.

Вести наблюдение за состоянием антивирусного контроля в организации.

Контролировать информацию, передаваемую по электронной почте, с целью исключения утечки конфиденциальной информации по открытым каналам связи в Учреждении.

Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

Периодически представлять руководству отчет о состоянии защиты и о нештатных ситуациях на объектах АИС и допущенных пользователями нарушениях установленных требований по защите информации.

Вносить предложения для принятия решений о привлечении виновных к ответственности, за грубые нарушения требований нормативных документов по обеспечению сохранности конфиденциальной информации, а также о приостановке работ в случае обнаружения условий для утечки информации или материалов с пометкой для служебного пользования.

3. **Права ответственного за информационную безопасность Ответственный за информационную безопасность имеет право:**

Проводить мероприятия по защите конфиденциальной информации от

Несанкционированного доступа.

Требовать от сотрудников Учреждения соблюдения установленных технологий обработки информации и выполнения инструкций по защите информации.

Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АИС.

Обращаться к руководителю Учреждения с требованием прекращения работы в АИС при несоблюдении установленной технологии обработки информации и невыполнении требований по защите информации пользователями.

Отключать от сети пользователей, осуществивших НСД к защищаемым ресурсам ЛВС и БД или нарушивших другие требования по безопасности информации.

Запрещать устанавливать на серверах и рабочих станциях ЛВС нештатное программное и аппаратное обеспечение. Ответственность лица, ответственного за информационную безопасность

Ответственный за информационную безопасность несет ответственность за качественное и своевременное выполнение задач, возложенных на него и изложенных в настоящей инструкции, а также определенных в текущих приказах и распоряжениях руководителя Детского сада

На ответственного за информационную безопасность возлагается персональная ответственность за программно-технические и криптографические средства защиты информации, и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.