муниципальное дошкольное образовательное учреждение
«Детский сад № 189 Центрального района Волгограда »
400066, Волгоград, ул. Краснознаменская д.21: тел.(8442) 33-46-68,e-mail: dou189@volgadmin.ru

СОГЛАСОВАНО
Председатель трудового коллектива
_____ О.В.Лобачева

УТВЕРЖДЕНО
Заведующий МОУ Детский сад № 189
_____О.К.Кириличева

Протокол № _1__от 09.01.2023г.

Приказ № 3_от 09.01.2023г.

МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ " ДЕТСКИЙ САД № 189 ЦЕНТРАЛЬНОГО РАЙОНА ВОЛГОГРАДА"

Подписан: МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "ДЕТСКИЙ САД № 189 ЦЕНТРАЛЬНОГО РАЙОНА ВОЛГОГРАДА" DN: ИНН=003444112343, СНИЛС=01544987060, ОГРН=1043400311096, STREET="Краснознаменская, 21", E=dou189@volgadmin.ru, C=RU, S=Волгоградская область, L=Волгоград, O="МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "" ДЕТСКИЙ САД № 189 ЦЕНТРАЛЬНОГО РАЙОНА ВОЛГОГРАДА"", G=Ольга Константиновна, SN=Кириличева, T=Заведующий, CN="" МУНИЦИПАЛЬНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ""ДЕТСКИЙ САД № 189 ЦЕНТРАЛЬНОГО РАЙОНА ВОЛГОГРАДА""
Основание: Я являюсь автором этого документа
Местоположение: место подписания
Дата: 2023-02-09 18:19:26
Foxit Reader Версия: 10.0.0

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

Ответственного за информационную безопасность и внедрение системы контентной фильтрации МОУ Детский сад № 189

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет основные обязанности и ответственность лица за информационную безопасность муниципального дошкольного учреждения «Детский сад № 189 Центрального района Волгограда» (далее- Учреждение).

1.2. Ответственный за информационную безопасность назначается приказом руководителя Учреждения.

1.3. 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 модернизации и эксплуатации АИС.

1.4. 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 Учрежления и информации, циркулирующей в них.

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

1.6. Инструкция реулирует отношения между ответственным за информационную безопасность, пользователями АИС, сторонними организациями, возникающие при ;

- эксплуатации и 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.

1.7.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 средствами защиты.

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

2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Ответственный за информационную безопасность обязан;

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

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

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

2.4. Организовать сопровождение работ по категорированию объектов средств вычислительтной техники Учреждения.

2.5.Знать перечень установленных в подразделениях Учреждения серверов, рабочих станций, средств контрольно-множественной техники и топологию локально-вычислительной сети.

2.6. Иметь перечень информационных ресурсов Учреждения.

2.7. Обеспечить доступ к защищаемой информации пользователя АИС согласно их прав доступа при получении оформленного соответствующим образом разрешения.

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

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

2.10.Не допускать установку, использование, хранение и размножение АИС.

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

2.12.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.

2.13. Контролировать физическую сохранность средств и оборудования АИС.

2.14.Присутствовать при внесении изменений в конфигурацию(модификацию) аппаратно-программны средств защищенных рабочих станций и серверов.

2.15. Участвовать в приемке новых программных и аппартных средств.

2.16. Периодически проверять состояние используемых СЗИ НСД и осуществлять проверку правильности их настройки.

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

2.18. Вести контроль за процессом резервирования и дублирования важных ресурсов АИС.

2.19.Вести наблюдение за состоянием антивирусного контроля в организации.

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

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

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

2.23.Вносить предложения для принятия решений о привлечении виновных к ответственности за грубые нарушения требований нормативных документов по обеспечению сохранности конфиденциальтной информации, а также о приостановке ракбот 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;

3.1.Проводить мероприятия по защите конфиденциальной информации от несанкционированного доступа.

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

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

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

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

3.6. Запрещать устанавливать на серверах и рабочих станциях ЛВС нештатное программное и аппаратное обеспечение.

4. ОТВЕТСТВЕННОСТЬ ЛИЦА ОТВЕТСТВЕННОГО ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

4.1.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.

4.2. 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.