ПРИНЯТО:
на общем собрании трудового коллектива
Протокол № 1____
От 12.01.2026 г.

УТВЕРЖДАЮ:
Заведующий МБДОУ «Детский сад комбинированного вида № 12» НМР РТ
_____ Е.Н.Мутигуллина
Приказ № 19/01 от 12.01.2026г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0E14A3308F7CC8DA87E36413DEC60026
Владелец: Мутигуллина Елена Накиповна
Действителен: с 17.04.2025 до 11.07.2026

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ (ИСПДн)

в муниципальном бюджетном дошкольном образовательном учреждении
«Детский сад комбинированного вида № 12»
Нижнекамского муниципального района Республики Татарстан

Настоящий документ подготовлен в рамках выполнения работ по обеспечению безопасной эксплуатации информационной системы персональных данных (далее - ИСПДн) в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад комбинированного вида № 12» Нижнекамского муниципального района Республики Татарстан (далее - ДОУ).

1. Общие положения

1.1. Пользователь ИСПДн (далее - Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных ДОУ.

1.2. Пользователем является каждый работник ДОУ, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о защите персональных данных и другими регламентирующими документами ДОУ.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования настоящей Инструкции и других внутренних распоряжений, регламентирующих порядок действий по защите персональных данных.

2.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению

1

безопасности ПДн, а также руководящих и организационно- распорядительных документов.

1.1. Соблюдать требования парольной политики (раздел 3).

1.2. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других (раздел 4).

1.3. Обо всех выявленных нарушениях, связанных с информационной безопасностью ДОУ, а также для получения консультаций по вопросам информационной безопасности необходимо обратиться к администрации ДОУ.

1.4. *Пользователям запрещается*:

-разглашать защищаемую информацию третьим лицам;

-копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

-самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

-несанкционированно открывать общий доступ к папкам на своей рабочей станции;

-отключать (блокировать) средства защиты информации;

-обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

-сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

-привлекать посторонних лиц для производства ремонта или настройки АРМ без согласования с ответственным за организацию работы с ПД.

1.5. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <CtrlxAlt><Del> и выбрать опцию <Блокировка>.

1.6. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

2. Организация парольной защиты

2.1. Полная плановая смена паролей в ИСПДн проводится по мере необходимости, но не реже одного раза в год.

2.2. Правила формирования пароля:

-пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

-пароль должен состоять не менее чем из 8 символов;

-в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z; б) строчные буквы английского алфавита от a до z; в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

-запрещается использовать в качестве пароля имя входа в систему, простые пароли типа "123", "111", "qwerty" и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних

животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

-запрещается использовать в качестве пароля один и тот же повторяющийся символ

либо повторяющуюся комбинацию из нескольких символов;

-запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

-запрещается выбирать пароли, которые уже использовались ранее.

2.3. Правила ввода пароля:

-ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

-во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамерами и др.).

2.4. Правила хранения пароля:

запрещается записывать пароли на бумаге, в файле, в электронной записной книжке и на других носителях информации, в том числе на предметах;

запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

2.5. Лица, использующие паролирование, обязаны:

-четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

-своевременно сообщать ответственным за организацию работы с ПД об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3. Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и (или) международного обмена (сети "Интернет" и других) (далее - Сеть) на элементах ИСПДн должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

осуществлять работу при отключенных средствах защиты (антивирусах и других);

передавать по Сети защищаемую информацию без использования средств шифрования;

посещать сайты сомнительной репутации (порносайты, сайты, содержащие нелегально распространяемое ПО, и другие).