ДОКУМЕНТ ПОДПИСАН ПРОСТОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Документ отправлен на официальный сайт: sosh2.obmizhn.ru
Уполномоченное лицо – руководитель образовательного учреждения:
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "НИЖНЕГОРСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №2" НИЖНЕГОРСКОГО РАЙОНА РЕСПУБЛИКИ КРЫМ
Действителен с: с 05.08.2026, 14:17
Действителен до: до 29.10.2027, 14:17
Ключ подписи: 00EA8A9CBA0690E6D6C9ABFEDBD28FE47

Муниципальное бюджетное общеобразовательное учреждение «Нижнегорская средняя общеобразовательная школа №2» Нижнегорского района Республики Крым

УТВЕРЖДЕНЫ
приказом МБОУ «Нижнегорская СОШ №2»
от «08» октября 2026г. № 484

ПРАВИЛА
управления доступом к государственной информационной системе сферы образования Республики Крым

1. Общие положения

1.1. Настоящие Правила устанавливают порядок предоставления, изменения, приостановления и прекращения доступа работников образовательной организации к государственной информационной системе сферы образования Республики Крым (далее — ГИС) и разработаны в соответствии с приказом ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» и письмом Министерства образования, науки и молодёжи Республики Крым от 6 октября 2026 г. № 7776/01-15.

1.2. Доступ к ГИС осуществляется исключительно посредством единой системы идентификации и аутентификации (далее — ЕСИА). Учётная запись пользователя ГИС привязана к учётным данным ЕСИА, в силу чего компрометация учётных данных работника влечёт получение доступа к функциям, закреплённым за его ролью.

1.3. Администратор образовательной организации в ГИС не является владельцем или оператором системы и обладает правами только в пределах своей организации.

1.4. Правила обязательны для всех работников, допущенных к работе в ГИС.

2. Принципы управления доступом

— минимум прав: работнику предоставляется объём прав, необходимый исключительно для исполнения его должностных обязанностей;

— персонификация: каждая учётная запись закрепляется за одним работником; групповые и обезличенные учётные записи не допускаются;

— разделение ролей: совмещение в рамках одной привилегированной учётной записи ролей системного администрирования и ролей администратора безопасности не допускается; ответственный за выявление инцидентов и реагирование на них не может быть администратором ГИС;

— документальное основание: предоставление, изменение и прекращение прав администратора оформляется приказом руководителя;

— усиленная аутентификация: для всех учётных записей с расширенными правами обязательна двухфакторная аутентификация в ЕСИА;

— доверенное устройство: вход в ГИС допускается только с рабочих станций, включённых в утверждённый перечень; вход с личных и незарегистрированных устройств запрещён.

3. Роли и права доступа (матрица доступа)

Роль	Права в ГИС	Кому назначается	Основание назначения	2ФА ЕСИА
Администратор образовательной организации	создание, изменение и блокирование учётных записей работников, обучающихся и законных представителей; назначение и изменение ролей; экспорт данных; управление структурой классов и списочным составом	работник, определённый приказом; не более двух лиц	приказ руководителя	обязательна
Ответственный за информационную безопасность	просмотр журналов событий и действий учётных записей; инициирование блокировки учётной записи; без прав администрирования	работник, не являющийся администратором ГИС	приказ руководителя	обязательна
Заместитель руководителя (учебная работа)	просмотр и выгрузка отчётов по организации; без управления учётными записями	по должности	приказ руководителя	обязательна
Классный руководитель	ведение журнала и дневника своего класса; просмотр данных обучающихся класса	по должности	должностная инструкция	рекомендуется
Педагогический работник	ведение журнала по своим предметам и классам	по должности	должностная инструкция	рекомендуется
Иные работники	доступ не предоставляется	—	—	—

Матрица заполняется под фактическую структуру организации. Строки, не применимые к организации, удаляются; добавление роли возможно только с указанием основания назначения.

4. Порядок предоставления и прекращения доступа

4.1. Доступ предоставляется на основании заявки непосредственного руководителя работника, согласованной ответственным за информационную безопасность. Права администратора предоставляются только приказом руководителя.

4.2. Работник допускается к работе в ГИС после инструктажа и подписания листа ознакомления с настоящими Правилами.

4.3. Доступ прекращается в день прекращения трудовых отношений, перевода на должность, не требующую доступа, либо в день издания приказа об отзыве прав. Ответственный за информационную безопасность в тот же день блокирует учётную запись и отзывает активные сессии.

4.4. Доступ приостанавливается незамедлительно при компрометации учётных данных, выявлении признаков несанкционированного доступа, а также если владелец учётной записи с расширенными правами не прошёл настройку двухфакторной аутентификации — в этом случае права временно понижаются до уровня обычного пользователя.

5. Ревизия учётных записей

5.1. Ревизия состава учётных записей и объёма прав проводится не реже одного раза в квартал, а также незамедлительно после кадровых изменений и при выявлении инцидента. Результаты оформляются актом.

5.2. При ревизии проверяются: соответствие перечня администраторов приказу; наличие двухфакторной аутентификации у всех учётных записей с расширенными правами; отсутствие учётных записей уволенных работников; факты назначения и изменения ролей и массового экспорта данных за истекший период.

6. Обязанности и ответственность пользователя

— не передавать учётные данные третьим лицам, включая коллег;

— не вводить учётные данные ЕСИА на страницах, не являющихся официальными, в том числе на сайтах, имитирующих электронный журнал и страницы органов управления образованием;

— незамедлительно сообщать ответственному за информационную безопасность о подозрении на компрометацию учётных данных и о любых аномалиях в работе ГИС;

— не работать в ГИС с личных и незарегистрированных устройств.

Пользователь несёт персональную ответственность за сохранность своих учётных данных. Нарушение настоящих Правил является основанием для привлечения к дисциплинарной ответственности.

Ответственный за информационную безопасность

_____ _____Н.А.Возгрина_

(подпись) (инициалы, фамилия)

С Правилами ознакомлены:

№	Фамилия, имя, отчество	Должность	Дата	Подпись
1	Миколенко Снежана Александровна	Методист		
2	Яцута Анна Анатольевна	Секретарь учебной части		
3	Тюрина Елена Анатольевна	ассистент (помощник) по оказанию технической помощи инвалидам и лицам с ограниченными возможностями здоровья		
4				
5				
6				