Attesto

Обзор безопасности платформы

Документ сформирован: 01.08.2026

Attesto это платформа доказуемой аттестации по охране труда. Ниже описано, как мы защищаем доступ к платформе и данные пользователей.

Аутентификация и пароли

Пароли хранятся только в виде криптографического хеша (bcrypt). В открытом виде они не хранятся и недоступны никому, включая администраторов платформы. Сессия пользователя передается в подписанной httpOnly cookie, недоступной скриптам страницы, по умолчанию по защищенному соединению.

Разделение доступа по ролям

Действует ролевая модель: администратор, инженер по охране труда, работник и аудитор. Каждая роль видит и может делать только то, что положено ей, на уровне каждого запроса к серверу.

Изоляция данных между компаниями

Платформа многокомпанийная. Данные одной организации недоступны другой: при каждом обращении сервер проверяет принадлежность запрашиваемых данных к компании пользователя.

Шифрование канала и защитные заголовки

Весь трафик идет по HTTPS с автоматическим выпуском сертификатов. Включены защитные заголовки: строгий транспорт (HSTS), запрет встраивания страниц в чужие сайты, политика безопасности контента и запрет угадывания типов файлов.

Защита от перебора и злоупотреблений

Ограничение частоты запросов защищает вход и регистрацию от перебора паролей, а операции искусственного интеллекта от злоупотреблений. Серийные номера допусков не перечисляемы, что исключает подбор по публичной проверке.

Прокторинг и доказательность

На экзамене подтверждается личность сдающего (сравнение лица с эталонным фото) и фиксируются кадры. Кадры и фотографии хранятся в защищенном хранилище вне публичного доступа. Открыть их может только уполномоченный сотрудник той же компании.

Неизменяемый аудит действий

Ключевые действия фиксируются в журнале аудита. Это дает прослеживаемость для внутреннего разбора и проверки инспектором, а также защищает от незаметного изменения данных.

Хранение данных и искусственный интеллект

Данные размещаются на выделенном сервере и не передаются третьим лицам без необходимости. Генерация обучающего контента может выполняться локальной моделью на

сервере организации тогда регламенты и материалы компании не покидают ее периметр.

Ответственное раскрытие уязвимостей

Если вы нашли уязвимость, сообщите нам на security@attesto.kz. Мы рассмотрим обращение и устраним проблему.

> Этот документ описывает меры защиты, реализованные в платформе Attesto (внутренняя самооценка по результатам технического ревью кода). Документ не является независимой сертификацией. Независимый тест на проникновение и отраслевые сертификации (SOC 2, ISO 27001) находятся на дорожной карте.

attesto.kz security@attesto.kz