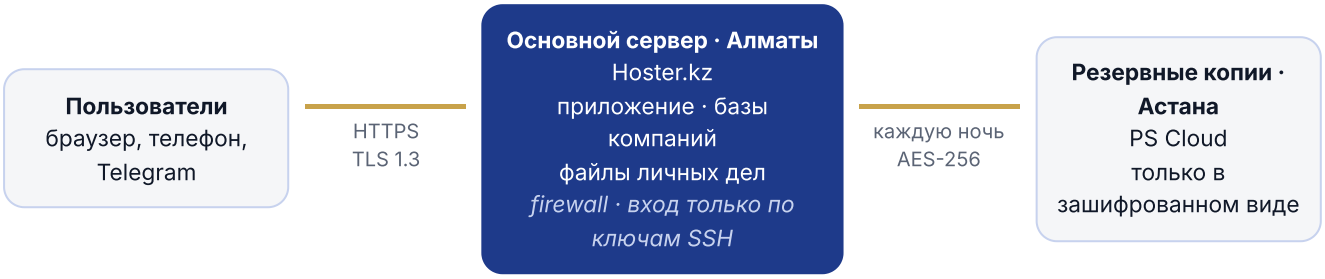
Система безопасности и размещение данных

Кратко. Сайт, базы данных всех компаний платформы и все файлы (личные дела, сканы документов, резюме) размещены на серверах в Республике Казахстан: основной сервер — в Алматы (Hoster.kz), зашифрованные резервные копии — в Астане (PS Cloud Services). Данные каждой компании хранятся в отдельной базе. Соединение с сайтом защищено TLS, вход — пароль и второй фактор, все действия с персональными данными записываются в журналы. Оператор персональных данных — компания-работодатель; Witstaff обрабатывает данные по её поручению.

1. Расположение инфраструктуры

Компонент	Провайдер и место	Что хранится / делает
Основной сервер РК	ТОО «Компания Hoster.KZ», дата-центр в г. Алматы; облачный сервер (4 vCPU, 16 ГБ, NVMe 200 ГБ), Ubuntu 24.04 LTS	Веб-приложение; базы данных всех компаний (отдельная база на каждую компанию) и база платформы; файлы личных дел, сканы, документы, резюме; журналы.
Резервные копии РК	PS Cloud Services (ps.kz), объектное хранилище, регион Астана (kz-ast-1)	Ежедневные зашифрованные копии баз, файлов и настроек. Другой провайдер и другой город, чем основной сервер.
Сервер проверки ЭЦП РК	Hoster.kz, отдельный облачный сервер	NCANode — проверка подписей ЭЦП НУЦ РК. Персональные данные не хранит; доступ только по ключу.
Домен witstaff.kz РК	Hoster.kz (регистратор и DNS)	Только записи, указывающие на серверы в РК, и записи почты. Данные пользователей через DNS не проходят.



2. Какие данные обрабатываются

- **Кадровые данные сотрудников и персонала:** ФИО, ИИН, дата рождения, контакты, адреса, данные удостоверения, должность, даты приёма и увольнения, отпуска, обучение и допуски, кадровые документы и их сканы.
- **Данные кандидатов:** резюме, контакты, ответы на уточняющие вопросы, результаты тестовых заданий и собеседований (в том числе записи, если компания их включила).
- **Сведения из государственных баз** (eGov через Biometric.kz): цифровые документы, адрес прописки, исполнительные производства — только после подтверждения самим человеком кодом из сообщения 1414 или в eGov Mobile; сведения об учёте в диспансерах — дополнительно при наличии письменного согласия работника.

- **Учётные записи пользователей платформы:** логин, роль, хэш пароля, настройки второго фактора, журнал входов и сеансов.

3. Изоляция данных компаний и разграничение доступа

- **Отдельная база данных на каждую компанию.** Данные разных компаний физически хранятся в разных файлах баз; запросы одной компании не могут обратиться к данным другой. Это проверяется автоматическими тестами.
- **Роли:** администратор, HR-менеджер, рекрутер, модератор, супервайзер и пользователь Заказчика, сотрудник. Каждая роль видит только свои разделы; Заказчик — только своих работников; сотрудник — только свой кабинет.
- Администратор компании может дополнительно закрывать отдельные разделы конкретным пользователям и скрывать зарплатные данные.
- Сведения о здоровье (учёт в диспансерах) доступны только HR и администратору; каждая проверка фиксируется с автором и временем.

4. Вход в систему

Мера	Как реализовано
Хранение паролей	Пароли не хранятся — только стойкий хэш scrypt с уникальной солью для каждого пользователя.
Второй фактор (2FA)	Код из приложения-аутентификатора (TOTP) или код в Telegram; одноразовые резервные коды. Компания может сделать 2FA обязательной для ролей с доступом к данным. Один аутентификатор действует во всех компаниях пользователя. Секреты 2FA хранятся зашифрованными (AES-256-GCM).
Защита от подбора	Ограничение попыток: по адресу — 20 за 15 минут; по учётной записи — нарастающая пауза до 15 минут; 5 неверных кодов — пауза 15 минут. Массовые ошибки входа — уведомление администраторам.
Сеансы	Подписанный токен (HMAC-SHA256) в cookie с флагами HttpOnly, Secure, SameSite; реестр сеансов на сервере — любой сеанс можно завершить; срок — 7 дней; «выйти на всех устройствах».
Вход по ЭЦП	Ключом ЭЦП НУЦ РК через NCALayer или в eGov Mobile: человек подписывает одноразовую строку (3 минуты, повторно не принимается), подпись и отзыв сертификата проверяет NCANode, вход — по ИИН из сертификата. Засчитывается как вход со вторым фактором.
Сотрудники	Вход без пароля: одноразовый 6-значный код по ИИН, номеру телефона или e-mail. Код приходит SMS на номер из карточки, в Telegram или на e-mail; действует 5 минут, не больше 5 попыток. Только для роли «Сотрудник»: офисные роли (HR, рекрутеры, администраторы) входят паролем и вторым фактором.

5. Шифрование

- **При передаче:** только HTTPS — TLS 1.3 (TLS 1.2 — для старых устройств), сертификаты Let's Encrypt с автоматическим продлением, HSTS на 2 года: браузер не допускает незащищённое соединение.
- **Резервные копии** шифруются на сервере до отправки (restic, AES-256); хранилище PS Cloud получает только зашифрованные данные. Пароль шифрования хранится у владельца платформы.

- **Секретные ключи интеграций** (eGov, ИИ, почта, SMS, Telegram) — в файле настроек сервера с доступом только у системной учётной записи приложения; в коде и репозитории их нет.
- Ссылки кандидатов в личный кабинет зашифрованы; ИИН кандидатов для входа в кабинет хранится в виде хэша.

6. Защита сервера и сети

- Firewall: открыты только порты 80/443 (сайт) и 22 (администрирование).
- Администрирование только по ключам SSH; вход по паролю отключён; защита от подбора fail2ban.
- Автоматическая установка обновлений безопасности операционной системы.
- Приложение работает от отдельной системной учётной записи без прав администратора, с ограничениями systemd: запись только в свои каталоги, без доступа к домашним каталогам.
- База данных и приложение недоступны из интернета напрямую — только через веб-сервер Caddy.
- Обновления выкладываются с проверкой и автоматическим возвратом прежней версии при сбое.

7. Защита веб-приложения

- Политика безопасности содержимого (CSP): скрипты и шрифты только с собственного сайта; запрет встраивания сайта в чужие страницы (X-Frame-Options: DENY, frame-ancestors 'none'), nosniff, ограничение Referrer.
- Проверка всех входящих данных на сервере; проверка типа загружаемых файлов по содержимому; ограничения размера; защита от подделки запросов (CSRF).
- Сайт закрыт от индексации поисковыми системами.
- Автоматические тесты (159 сценариев, в том числе доступ по ролям и изоляция компаний) перед каждым выпуском.

8. Персональные данные (Закон РК «О персональных данных и их защите»)

- **Роли.** Оператор (собственник) персональных данных — компания-работодатель или компания, ведущая подбор. Witstaff — обработчик: обрабатывает данные по её поручению и в её интересах.
- **Локализация:** базы, содержащие персональные данные, размещены на территории РК (раздел 1).
- **Согласия:** кандидат даёт согласие от имени компании, которая ведёт подбор, в том числе на трансграничную передачу (раздел 10); учёт согласий (цель, источник, дата), отзыв согласия.
- **Политика конфиденциальности** опубликована: www.witstaff.kz/privacy; контакт по вопросам ПДн — privacy@witstaff.kz.
- **Журнал доступа к ПДн:** кто и когда открывал карточку, выгружал данные. **Журнал действий:** входы, изменения, подписания, удаления — с пользователем, временем и IP-адресом.
- **Сроки хранения и уничтожение:** настраиваемые сроки; система показывает данные, подлежащие уничтожению (в том числе сканы после увольнения).
- Сведения из госбаз запрашиваются только с подтверждением самого человека; данные eGov отмечаются в карточке как достоверные.

9. Резервное копирование, мониторинг и восстановление

Параметр	Значение
Периодичность	Ежедневно в 02:30 (Алматы)
Состав	Согласованные снимки всех баз данных, все файлы, настройки сервера
Место	PS Cloud Services, Астана — другой провайдер и город, чем основной сервер
Шифрование	AES-256 на стороне сервера, ключ — у владельца платформы
Срок хранения	14 ежедневных, 8 еженедельных, 12 ежемесячных копий
Проверка восстановления	Автоматически раз в месяц: копия восстанавливается, проверяется целостность баз. Первая проверка — 11.11.2026, успешно.
Мониторинг	Каждые 5 минут: доступность сайта и служб, выполнение резервного копирования, место на диске и нагрузка сервера; оповещения администратору в Telegram.

10. Внешние сервисы

Для отдельных функций платформа обращается к внешним сервисам. Данные в них не хранятся как в базе платформы, но передаются для обработки:

Сервис	Где	Для чего и какие данные
Biometric.kz (eGov)	РК	Цифровые документы, адрес прописки, исполнительные производства, учёт в диспансерах — по ИИН, с подтверждением человека.
SIGEX (sigex.kz)	РК	Подписание документов и вход через eGov Mobile по QR-коду: подписываемые данные и подпись.
Mobizon	РК	SMS с кодами входа и подписания: номер телефона и текст SMS.
hh.kz / hh.ru	РК / РФ	Публикация вакансий и получение откликов (данные кандидатов, откликнувшихся на hh).
Anthropic (Claude)	за рубежом (США)	ИИ-функции: разбор резюме и сканов, оценка кандидатов, разбор личных дел, помощник. Данные передаются только при использовании этих функций; по условиям коммерческого API не используются для обучения моделей.
Resend	за рубежом (США)	Доставка писем (уведомления, приглашения, коды, восстановление пароля): адрес и текст письма.
Daily.co	за рубежом (США)	Видеособеседования: видеосвязь, по выбору компании — запись и расшифровка.
Telegram	за рубежом	Уведомления, коды входа и кабинет сотрудника для тех, кто подключил бота.

Использование сервисов за рубежом означает трансграничную передачу отдельных персональных данных. Она отражена в согласии кандидата и в политике конфиденциальности; работодателю рекомендуется отразить её также в своём положении о персональных данных.

11. Ближайшие меры

- **Удаление прежних копий данных за рубежом.** До 11.11.2026 данные хранились у Vercel (файлы) и Turso (базы). После 1–2 недель стабильной работы на серверах в РК эти копии будут удалены (с предварительной резервной копией).

- **Обезличивание перед ИИ:** замена ИИН, номеров документов и контактов условными метками перед отправкой в ИИ-сервис.
- **Внешний мониторинг доступности** — проверка сайта с независимой площадки в дополнение к мониторингу на сервере.
- **Перевыпуск ключей интеграций**, передававшихся при настройке.

Документ описывает фактическое техническое состояние платформы Witstaff (ранее — TeamBuilder One) на 13.11.2026 и не является юридическим заключением о соответствии законодательству. Организационные меры (положение о ПДн, приказы о назначении ответственных, ознакомление сотрудников) оформляются компанией-оператором самостоятельно.