Wialon – ваш надежный телематический партнер

Wialon — это программное обеспечение для управления автопарком, которое контролирует миллионы транспортных средств по всему миру и помогает тысячам владельцев автопарков в их ежедневной работе.

Команда разработчиков Wialon делает все возможное для защиты ваших данных и данных ваших клиентов. Для нас безопасность данных – это больше, чем просто тренд или обязательное требование. Мы разрабатываем первоклассные защищенные продукты, применяя глобальные стандарты в области обеспечения качества, информационной безопасности и конфиденциальности.

Наши процессы организованы таким образом, чтобы гарантировать эффективное и своевременное внедрение лучших практик, связанных с менеджментом рисков, изменений, ресурсов, инцидентов и т. д.

Соответствие стандартам

Разработчик Wialon, компания Gurtam, придерживается Политики интегрированной системы менеджмента, что соответствует требованиям стандартов по менеджменту качества ISO 9001 и информационной безопасности ISO/IEC 27001. Это еще раз доказывает нацеленность компании Gurtam на поддержание высочайшего качества обслуживания и обеспечение конфиденциальности, целостности и доступности данных для всех наших партнёров.

Дата-центры Wialon

Дата-центры Wialon используют ультрасовременную IT-инфраструктуру, включая передовые технологии обработки и хранения информации. Все это дополнено автоматизированными процессами администрирования, которые обеспечивают эффективную защиту баз данных.

Wialon использует дата-центры категории защищенности Tier 3, что, помимо прочего, гарантирует время безотказной работы на уровне 99,5%.

Узнать больше

Откройте возможности платформы Wialon

Узнать больше

Комплексные меры безопасности

Для защиты ваших данных мы используем подход, который сформировался на основе многолетнего опыта. Он включает в себя предотвращение проблем с безопасностью, регулярное обучение команды и быстрое решение проблем при их возникновении.

Все указанные ниже политики доступны по запросу.

Осведомленность в вопросах информационной безопасности и конфиденциальности

Сразу после приема на работу каждый сотрудник обязан внимательно изучить наши политики и требования к информационной безопасности и впоследствии соблюдать их. Как минимум один раз в год все команда проходит внутреннее обучение по информационной безопасности и конфиденциальности. Специализированное углубленное обучение проходят те, кто занимает должности с расширенным доступом к данным — топ-менеджмент и разработчики программного обеспечения.

Управление правами доступа и разрешениями

Wialon определяет роли и в соответствии с ними обеспечивает ограничение доступа к ресурсам и активам. Это гарантирует разделение любых конфликтующих ролей для обеспечения максимальной объективности и результативности процесса. Предоставление доступа к ресурсам и активам компании основано на правиле «Запрещено все, что не разрешено». Мы определяем права доступа, руководствуясь принципом наименьших привилегий, а также принципами Need-to-know и Need-to-use.

Обеспечение безопасности при удаленной работе

Для повышения безопасности при удаленной работе мы используем такие меры и инструменты, как VPN, личные SSL-сертификаты, антивирусное программное обеспечение, надежные пароли, политики чистого рабочего стола и чистого экрана, автоматическую блокировку компьютера при бездействии, а также соблюдение правил ответственного использования информации.

Управление физической безопасностью

В офисах Wialon помещения разделены на отдельные зоны в зависимости от должностных обязанностей, а доступ в эти зоны контролируется с помощью идентификационных бейджей. Кроме того, доступ к оборудованию компании строго регламентирован, а также принимаются меры для защиты оборудования от внешних воздействий.

Обеспечение конфиденциальности данных

Вся информация, которой вы делитесь с Wialon, надежно защищена. Конфиденциальность информации обеспечивается различными техническими и организационными мерами, а также обязательным требованием к сотрудникам и третьим лицам подписывать NDA. Мы также внедрили стандарты GDPR в наши практики работы с данными. Чтобы обеспечить безопасное и ответственное обращение с личной информацией, мы регулярно проводим проверки безопасности в Wialon, следуя мировым стандартам.

Поддержание непрерывности операций

Wialon придерживается специальной политики и плана непрерывности операций, которые определяют RPO (Recovery Point Objective, или допустимую точку восстановления) и RTO (Recovery time objective, или допустимое время восстановления) для ключевых ИКТ-сервисов. Владельцы активов в соответствии с этим планом разработали планы аварийного восстановления, которые периодически тестируются и обновляются по мере необходимости. Wialon использует дата-центры Tier 3, которые играют ключевую роль в обеспечении бесперебойной работы и предоставлении качественных услуг. Кроме того, не реже одного раза в год мы проводим независимый пентест. Пожалуйста, свяжитесь с технической поддержкой Wialon, если вам нужно подтверждение проведения пентеста.

Разработка безопасного программного обеспечения

Наша команда применяет передовые подходы к разработке программного обеспечения. Мы отслеживаем ситуацию с различными уязвимостями и не реже одного раза в год проводим аудит безопасности аккредитованными сторонними компаниями. Мы уделяем первостепенное внимание качеству продукта, постоянно совершенствуем процессы и интегрируем меры информационной безопасности и конфиденциальности на каждом этапе жизненного цикла продукта.

Управление инцидентами

Основная цель управления инцидентами заключается в том, чтобы быстро восстановить деятельность при возникновении чрезвычайных ситуаций. Для этого Wialon определил роли, информационные каналы и процедуры классификации, реагирования, устранения последствий и предотвращения повторения инцидентов.

Управление рисками

Мы выявляем риски для активов на основе наличия конкретных угроз и связанных с ними уязвимостей. После оценки рисков мы разрабатываем стратегии управления и предлагаем меры по смягчению значительных рисков, которые могут включать улучшение текущих процессов или введение новых в ответ на выявленные возможности.

Ведение журнала и мониторинг

Мониторинг событий позволяет выявлять аномалии программного/системного оборудования и предотвращать угрозы. Для этого применяются анализ сотрудниками, разнообразные инструменты (например, Zabbix, noc.wialon.com) и аудиты. Владельцы активов определяют объем и частоту мониторинга и порядок хранения записей. Владельцы также управляют ведением журналов и оповещениями, обеспечивая регулярный мониторинг и своевременное реагирование.

Полезные ссылки

- Кодекс поведения поставщика
- Общий регламент технической поддержки
- Документация SDK/API
- Заявление о применимости
- Техническая поддержка Wialon
- Форум
- Wialon Network Operations Center
- Справочный центр Wialon

Если у вас есть потенциальные клиенты, которые интересуются политикой безопасности Wialon, обратитесь за помощью в команду Project Implementation.

Написать

Свяжитесь с нами

privacy@wialon.com

для вопросов, касающихся обработки персональных данных

infosec@wialon.com

для вопросов, связанных с информационной безопасностью и конфиденциальностью