Wialon, seu parceiro de software seguro

O Wialon é um software de gestão de frotas que rastreia milhões de veículos em todo o mundo, atendendo diariamente milhares de proprietários de frotas.

Nossa equipe por trás do Wialon se preocupa com a proteção dos seus dados e dos seus clientes, reconhecendo que a segurança não é apenas um uma tendência ou um requisito obrigatório. Nós desenvolvemos produtos seguros e de alto nível integrando continuamente padrões globais de garantia de qualidade, segurança da informação e privacidade.

Nossos processos são instituídos para garantir a implementação eficiente e oportuna das melhores práticas relacionadas à gestão de riscos, gestão de mudanças, gestão de recursos, gestão de incidentes, entre outros.

Compliance

A Gurtam, empresa que desenvolve o Wialon, segue uma política de sistema de gestão integrada que atende aos requisitos de gestão de qualidade do ISO 9001 e aos requisitos de segurança da informação do ISO/IEC 27001. Isto prova a dedicação da Gurtam em manter a mais alta qualidade de serviço e salvaguardar a confidencialidade, integridade e disponibilidade de dados para todos os nossos parceiros.

Data centers do Wialon

Os data centers do Wialon utilizam infraestrutura de TI de última geração, incorporando tecnologias avançadas para processamento e armazenamento de informações, além de serem complementados por processos automatizados, garantindo segurança completa do banco de dados.

O Wialon utiliza data centers Tier 3, o que garante, entre outras coisas, um uptime de 99,5%.

Saiba mais

Conheça as funcionalidades da plataforma Wialon

Saiba mais

Medidas completas de segurança

Para proteger os seus dados, utilizamos uma abordagem que evoluiu ao longo de nossos muitos anos de experiência e inclui a prevenção de problemas de segurança, a capacitação contínua de nossa equipe e a resolução rápida de problemas.

Todas as políticas mencionadas abaixo estão disponíveis mediante solicitação.

Segurança da informação e conscientização sobre privacidade

Ao serem contratados, todos os funcionários do Wialon são obrigados a ler e a cumprir nossas políticas e requisitos de segurança da informação. Pelo menos uma vez por ano são realizados treinamentos internos sobre segurança e privacidade da informação para toda a equipe. Treinamentos especializados e aprofundados também são fornecidos para cargos com acesso aprimorado a dados, como cargos de alta administração e desenvolvimento de software.

Gestão de acesso e permissões

O Wialon define funções e responsabilidades com acesso limitado a recursos e ativos. Isso garante que qualquer função confiantes sejam segregadas para maximizar a objetividade e a eficácia do processo. A concessão de acesso aos recursos e ativos da empresa baseia-se em "Tudo é proibido a menos que seja expressamente permitido". Determinamos os direitos de acesso com base no princípio do menor privilégio, bem como nas abordagens Precisa-saber e Precisa-usar.

Garantia de segurança no trabalho remoto

Para aumentar a segurança durante o trabalho remoto de nosso funcionários, empregamos medidas e ferramentas como VPN, certificados SSL, pessoais, software antivírus, senhas fortes, políticas de mesa e tela limpas, bloqueio automático do computador durante a inatividade e adesão às regras para o uso responsável das informações.

Gestão de segurança física

Nos escritórios do Wialon os espaços são segmentados em zonas distintas com base nas funções do trabalho, e o acesso a essas áreas é controlado através do uso de crachás de identificação. Além disso, o acesso aos equipamentos da empresa é estritamente regulamentado e existem medidas de proteção para evitar interferências externas nos equipamentos.

Garantindo a privacidade dos dados

Todas as informações que você compartilha com o Wialon são protegidas. A confidencialidade das informações é mantida por meio de diversas medidas técnicas e organizacionais, aliadas à obrigatoriedade de assinatura de NDAs por funcionários e terceiros. Também incorporamos os padrões GDPR em nossas práticas de dados. Para garantir que tratamos as informações pessoais de forma segura e responsável, realizamos regularmente verificações de segurança no Wialon, seguindo os padrões globais.

Manutenção da continuidade das operações

O Wialon tem uma política dedicada e um plano de continuidade que descreve o Recovery Point Objective (RPO) e o Recovery Time Objective (RTO) para os principais serviços de TIC. Os proprietários de ativos alinhados a esse plano desenvolveram planos de recuperação de desastres que são submetidos a testes periódicos e atualizados conforme necessário. O Wialon usa data centers Tier 3 que desempenham um papel crucial para garantir contínuas operações e prestação de serviços. Além disso, pelo menos uma vez por ano, um pentest de terceiros é realizado. Por favor, entre em contato com o suporte técnico do Wialon caso precise da confirmação do pentest.

Desenvolvimento seguro de software

Nossa equipe utiliza técnicas avançadas no desenvolvimento de nossos softwares. Monitoramos o cenário de diversas vulnerabilidades e passamos por auditorias de segurança realizadas por empresas terceirizadas certificadas pelo menos uma vez por ano. Priorizamos a qualidade do produto, refinamos consistentemente os processos de teste e integramos medidas de segurança e privacidade da informação em todas as fases do ciclo de vida do produto.

Gestão de Incidentes

O principal objetivo da gestão de incidentes é restaurar rapidamente as operações normais após emergências. Para fazer isso, o Wialon definiu funções, canais de informação e procedimentos para classificação de incidentes, resposta, eliminação de consequências e prevenção de recorrências.

Gestão de risco

Identificamos riscos a ativos com base na presença de uma ameaça específica e na vulnerabilidade relacionada. Após a avaliação dos riscos, elaboramos estratégias de gestão e propomos medidas de mitigação para riscos significativos, que podem envolver a melhoria dos processos atuais de SGI (Sistema de Gestão de Informação) ou a introdução de novos processos em resposta ao que foi identificado.

Registro e monitoramento

O monitoramento de eventos detecta anormalidades no software/sistema e evita ameaças através de análises de funcionários, ferramentas (por exemplo, Zabbix, noc.wialon.com) e auditorias. Os proprietários dos ativos definem o escopo do monitoramento, a frequência e o armazenamento dos registros. Eles também gerenciam registros e alertas, garantindo monitoramento e resposta regulares.

Links úteis

- Código de Conduta de Fornecedores
- Declaração de Aplicabilidade
- Centro de Operações da Rede do Wialon
- Regulamentações de suporte técnico
- Suporte técnico no Wialon
- Help center Wialon
- Documentação de SDK/API
- Fórum

Se você tem clientes potenciais interessados na segurança do Wialon, entre em contato com nosso Project Implementation team para receber assistência.

Entre em contato

Entre em contato

privacy@wialon.com

para questões relativas à utilização de dados pessoais

infosec@wialon.com

para questões relacionadas à segurança e privacidade da informação