Acquisitie, ontwikkeling en onderhoud van systemen

Wij zijn een softwarebedrijf en daarom vereisen de beveiliging en betrouwbaarheid van al onze producten een veilige codering en processen die een flexibele productlevensduur waarborgen.

Onze Secure Software Development Life Cycle omvat:

- Peer-reviewed design en codering
- Stijlrichtlijnen
- Kwaliteitscontroles op functionaliteit/belastingstests
- Release- en veranderingsmanagement
- Reviews van statische codes (OWASP Top 10 / SANS Top 25)

Daarnaast faciliteren we de volgende programma's om veilige engineering te garanderen:

- Beveiligingstraining voor ons personeel
- Beveiligingstests en -controles op implementatieniveau
- Robuust maken van systeem
- Kwetsbaarheids-/patchbeheer
- Beveiligingstests webapplicaties

Engineering

Analyse software-design

Voltooide ontwikkeling

Statische inspectie van de code

Kwaliteits-controle

Dynamische analyse van de applicatie

Implementatie

Implementatie en stabilisatie van de applicatie

Relaties met leveranciers

Door externe bedreigingen aan de rand van ons werkgebied te beheren, zorgen we ervoor dat het bedrijf geen extra risico's loopt via onze partners of leveranciers. Waar mogelijk selecteren we leveranciers die een internationale nalevingsstandaard voor informatieveiligheid aanhouden en/of dezelfde waarden in acht nemen als Webfleet Solutions met betrekking tot de bescherming van informatie en gegevensprivacy.

Informatiebeveiligingsincidenten

Bij beveiligingsincidenten is een effectieve aanpakstrategie essentieel. Hieronder vallen de communicatie met alle betrokken partijen en rapportage over zwakke plekken in de interne beveiliging ter ondersteuning van de veiligheid, zoals omschreven in verschillende wettelijke, regelgevende en contractuele overeenkomsten die hiervoor van kracht zijn.

Informatiebeveiligingsaspecten van Business Continuity Management

Ons gedetailleerde Business and Information Security Continuity-programma zorgt ervoor dat het Webfleet Solutions-serviceplatform zelfs in noodscenario's beschikbaar blijft voor onze klanten. Door onze actief-datacenterconfiguratie wordt de kans op een groot probleem in beide centra onwaarschijnlijk, omdat elk center indien nodig onze volledige bewerkingen kan handhaven. Dit houdt in dat u erop kunt rekenen dat het platform beschikbaar is wanneer u dit nodig hebt.

NALEVING EN GEGEVENSPRIVACY

Webfleet Solutions wordt gecontroleerd en getoetst door onze Data Privacy Officer (DPO) om naleving van de algemene verordening gegevensbescherming (AVG) en alle relevante lokale privacywetten te garanderen.

Ons Information Security Management System (ISMS)-team controleert regelmatig de wettelijke vereisten en beveiligingsvereisten die mogelijk van invloed zijn op het telematicaplatform of de gegevens die onder ISMS vallen.

HIGHLIGHTS

- **MAXIMALE BEVEILIGING EN INTEGRITEIT**
  Uw gegevens zijn veilig met ons ISO 27001-gecertificeerde systeem.
- **BESCHERMING VAN BESTUURDERSPRIVACY**
  Met onze focus op gegevensbescherming hebben we samengewerkt met gegevensprivacygroepen en werkgroepen om onze toewijding aan uw privacy te demonstreren.
- **VERWIJDERING VAN GEGEVENS**
  Gegevens worden gemarkeerd als 'dereferenced' en worden overschreven in het geval dat gegevens worden verwijderd. Dit wordt gedaan om te voorkomen dat de gegevens worden hersteld door andere partijen.
- **GEGEVENSBEHOUD**
  We behouden standaard alle gedetailleerde gegevens, waaronder nauwkeurige gegevenstracks tot maximaal negentig (90) dagen plus het logboek, dashboard en onze rapportage voor het huidige jaar en de afgelopen twee (2) jaar. Dit kan verschillen per landspecifieke regelgeving.
- **KIES INTEGRITEIT EN BESCHERM HET MILIEU**
  Wij leveren ons aandeel met een veilig platform waarmee u kosten kunt besparen en tegelijkertijd uw steentje bijdraagt aan beter milieu.

webfleet solutions
a Bridgestone company

GECERTIFICEERDE INFORMATIEBEVEILIGING EN GEGEVENSPRIVACY

Wilt u meer gedetailleerde technische informatie over beveiliging en gegevensprivacy? Vraag dan het whitepaper over gecertificeerde informatiebescherming en gegevensprivacy aan op de Webfleet Solutions-website op **www.webfleet.com**

Contact opnemen:
privacy@webfleet.com

webfleet solutions

BIJ WEBFLEET SOLUTIONS ZIJN WE GECOMMITTEERD AAN DE **BEVEILIGING EN PRIVACY VAN GEGEVENS.**

We investeren voortdurend in onze engineering, bewezen technologieën, processen en mensen om ervoor te zorgen dat we altijd het meest betrouwbare telematica-serviceplatform op de markt zijn.

DE KRACHT VAN HET WEBFLEET SOLUTIONS-SERVICEPLATFORM

ISO/IEC 27001:2013 INFORMATION SECURITY-GECERTIFICEERD
Ons serviceplatform en onze volgroeide processen zijn gecertificeerd om onze klanten te garanderen dat ze kunnen profiteren van de hoogste standaard op het gebied van informatiebeveiliging en gegevensprivacy

HOOGSTE STANDAARD IN EV SSL-ENCRYPTIE
Veilig, versleuteld aanmelden en veilige, versleutelde gegevensoverdracht naar ons serviceplatform. U kunt erop vertrouwen dat uw gegevens veilig zijn

LOKALE INSTALLATIE
Nationale en internationale installatiespecialisten

EERSTEKLAS ONDERSTEUNING
Van lokale verkopers en systeemintegrators

APP CENTER
Bewezen integraties en invoegapplicaties beschikbaar in het App Center

Het is dan ook geen verrassing dat wij wereldwijd toonaangevend zijn op het gebied van fleet management en telematica.

Als een van 's werelds grootste leveranciers van telematicaservices, is deze voortdurende investering in onze dienstverlening belangrijk om zodoende de best mogelijke partner te zijn voor uw bedrijf - nu en in de toekomst.

ISO 27001-gecertificeerd

Ons Information Security Management System (ISMS) omvat alle kritieke bedrijfsprocessen die nodig zijn om de gegevens van het Webfleet Solutions-serviceplatform te beveiligen. Hier vallen onder andere architectuur, engineering, kwaliteitscontrole en IT-services onder die worden geleverd aan Webfleet Solutions BV bij onze technologiedivisie in Duitsland, evenals onze beveiligde datacenter-co-locaties in de Europese Unie. Dit is overeenkomstig de ISO/IEC 27001:2013-standaard en geïmplementeerd zoals beschreven in onze Statement of Applicability, versie van november 2016.

"De ISO 27001-certificering benadrukt dat we volledig controle hebben over onze processen en, nog belangrijker, dat onze klantgegevens in veilige handen zijn. Dit is cruciaal voor ons in onze levering van een bedrijfskritieke fleet management SaaS-oplossing ('Software as a Service')."

Thomas Schmidt, Managing Director, Webfleet Solutions

Beheersysteem informatiebeveiliging

De basis voor de toewijding van Webfleet Solutions aan informatiebeveiliging is onze reeks beveiligingsbeleidsregels en -programma's die de organisatie en het beheer van informatiebeveiliging dekken. Op basis van ons strikte risicobeheerprogramma dat is afgestemd op onze zakelijke doelstellingen, wordt een goed afgebakende veiligheidszone gehanteerd binnen het bereik van het ISMS, inclusief maar niet beperkt tot de volgende onderwerpen:

BELEID INZAKE INFORMATIEBEVEILIGING
Een gedetailleerde reeks beveiligingsbeleidsregels die zijn ontworpen om richting te geven aan het management en ondersteuning te bieden voor het informatiebeheersysteem en alle operationele activiteiten die verband houden met het Webfleet Solutions-serviceplatform.

ORGANISATIE VAN INFORMATIEBEVEILIGING
Informatiebeveiliging is belangrijk voor iedereen.
De rollen en verantwoordelijkheden van alle werknemers zijn gebaseerd op informatiebeveiliging. Samen met een fulltime informatiebeveiligingsteam zorgt iedereen voor naleving en governance van ISO 27001, en passen we ons aan de algemene verordening gegevensbescherming (AVG) en alle relevante lokale privacywetten aan.

BEVEILIGING VAN HUMAN RESOURCES
Informatiebeveiliging is cruciaal voor, gedurende en na de beëindiging van een dienstverband. Hieronder valt het selecteren van de juiste werknemers en het aanbieden van voortdurende persoonlijke training.

ASSET MANAGEMENT
Inventarisatie, eigendom en onderhoud tijdens de levensduur van een asset om ervoor te zorgen dat alle assets worden gecategoriseerd, gelabeld en toegewezen aan risico-eigenaars. Hieronder valt de veilige afhandeling van intellectueel eigendom en klantgegevens van het bedrijf.

TOEGANGSCONTROLE
Via identiteitsbeheer wordt alle toegang beperkt tot een 'need-to-have'- en 'need-to-know'-basis. Extra instellingen helpen om onbevoegde toegang te voorkomen. Systeemregistratie en -controle biedt bijvoorbeeld realtime detectie in het gehele beveiligingsspectrum.

CRYPTOGRAFIE
We investeren in ultramoderne hardware- en softwareoplossingen. Bewezen cryptografietechnologieën beschermen de vertrouwelijkheid en integriteit van de gegevens van onze klanten en onze bedrijfssystemen.

FYSIEKE BEVEILIGING EN OMGEVINGSBEVEILIGING
We hebben twee onafhankelijke Tier3+-datacenters in de Europese Unie vanwege de strikte gegevensprivacyvereisten. Onze bewezen actief/actief-configuratie zorgt voor herstel in noodscenario's en heeft hoge beschikbaarheidsmogelijkheden die regelmatig worden getest.

OPERATIONELE VEILIGHEID
We proberen een beheerd, strikt en herhaalbaar proces in onze werkzaamheden te behouden. Door een beveiligingsstandaard aan te houden, worden risicolevels beheerd en kunnen we effectief werken.

Highlights operationele veiligheid:

- **Operationele procedures en documentatie**
- **Back-up/hersteltests van kritieke systemen**
- **Controle van operationele omgevingen**
- **Incident-, probleem- en veranderingsmanagement gebaseerd op best practices**
- **Capaciteitsmanagement, waaronder belastingstests**
- **Scheiding van werkzaamheden**
- **Robuust maken van systeem**
- **Scheiding van omgevingen voor ontwikkeling, testen en productie**
- **Scannen op kwetsbaarheden**
- **Penetratietests**
- **Patchbeheer**

COMMUNICATIEVEILIGHEID
De beveiliging van gegevens die 'onderweg' zijn, vereist een veilig netwerk waar de gegevens door kunnen stromen. We gebruiken veilige communicatiemethoden zoals:

- **Netwerkscheiding**
- **VLAN-scheiding, DMZ met firewalls op meerdere niveaus**
- **Netwerktoegangscontrole (NAC)**
- **Standaardversleuteling op basis van de laatste industriestandaard**