Akvizice, vývoj a údržba systémů

Jelikož jsme softwarovou firmou, bezpečnost a spolehlivost všech našich produktů je závislá na bezpečných kódovacích principech a postupech, aby byla zajištěna aktivní životnost produktů.

Náš životní cyklus vývoje bezpečného softwaru. zahrnuje:

- Kontrolovaný design a kódování
- Zásady týkající se stylu
- Funkční kontrolu kvality / zátěžové testování
- Řízení vydaných verzí a změn
- Hodnocení statického kódu (OWASP Top 10 / SANS Top 25)

K zabezpečení našeho inženýrského okruhu používáme dále následující programy:

- Vzdělávání v oblasti zabezpečení pro naše pracovníky
- Kontroly a testování zabezpečení na úrovni implementace
- Hardening (zabezpečení) systémů
- Správa zranitelných míst / oprav
- Testování zabezpečení webových aplikací

Inženýrství	Dokončený vývoj	Zajištění kvality	Nasazení
Návrh analýzy softwaru	Statická inspekce kódu	Dynamická analýza aplikace	Nasazení a stabilizace aplikace

Vztahy s dodavateli

Zabezpečení vnějších hrozeb na hranici našeho dosahu pomáhá zaručit, že naši partneři a dodavatelé nepřinesou naší organizaci žádná další rizika. Pokud je to možné, vybíráme dodavatele, kteří dodržují mezinárodní normu o zabezpečení informací anebo vyznávají podobné hodnoty jako společnost Webfleet Solutions týkající se ochrany informací a soukromí dat.

Správa informačních bezpečnostních událostí

Pokud dojde k narušení bezpečnosti, je důležité zvolit efektivní přístup k jejímu řešení. Tento proces zahrnuje včasnou komunikaci se všemi zúčastněnými stranami a nahlášení všech slabých stránek interního zabezpečení sloužícího k podpoře bezpečnostní zóny na základě požadavků různých legislativních, regulačních a smluvních dohod platných v místě oznámení.

Aspekty zabezpečení informací pro správu celistvosti firmy

Provozujeme detailní program celistvosti firemního a informačního zabezpečení, abychom našim zákazníkům zajistili dostupnost platformy služby Webfleet Solutions i v případě havárie. Díky naší konfiguraci datových center formou „aktivní/aktivní“ je pravděpodobnost významné havárie v obou centrech mizivá. Každé z center je v případě potřeby schopné pokrýt všechny naše operace. Znamená to, že se v případě potřeby můžete spolehnout na dostupnost platformy.

DODRŽOVÁNÍ A OCHRANA SOUKROMÝCH DAT

Společnost Webfleet Solutions je kontrolována a auditována naším pracovníkem ochrany soukromí osobních údajů (DPO), aby bylo zajištěno dodržování obecného nařízení o ochraně osobních údajů vydaným EU i dalších příslušných místních právních předpisů na ochranu soukromí.

Náš tým pro systém správy zabezpečení informací (ISMS) provádí pravidelné kontroly bezpečnostních požadavků, kterou mohou mít vliv na naši platformu telematických služeb nebo na informační prostředky v rámci systému ISMS.

NEJDŮLEŽITĚJŠÍ ÚDAJE

- **MAXIMÁLNÍ ZABEZPEČENÍ A INTEGRITA**
  S naším systémem s certifikací ISO 27001 jsou vaše data v bezpečí.
- **OCHRANA SOUKROMÍ ŘIDIČŮ**
  Ohledně našeho zaměření na ochranu dat jsme spolupracovali se skupinami a pracovními poradními sbory, které se touto problematikou zabývají, abychom prokázali svůj závazek vůči vašemu soukromí.
- **ODSTRANĚNÍ DAT**
  V případě odstranění dat se data označí jako dereferencovaná a přepíšou se, aby se zabránilo tomu, že budou obnovena neoprávněnými stranami.
- **UCHOVÁVÁNÍ DAT**
  Standardně uchováváme veškeré podrobné údaje včetně přesných datových stop po dobu až devadesáti (90) dnů pro aktuální rok a předchozí dva (2) roky pro vaši knihu jízd, řídicí panel a hlášení. To se může lišit v závislosti na souvisejících předpisech konkrétních zemí.
- **VYBERTE SI INTEGRITU, CHRAŇTE ŽIVOTNÍ PROSTŘEDÍ**
  Děláme, co je v našich silách, abychom vám poskytli bezpečnou platformu, která vám umožní snížit náklady a zároveň chránit životní prostředí.

webfleet solutions
a Bridgestone company

Máte zájem o podrobnější technické informace týkající se zabezpečení informací a soukromí dat? Dokument o certifikovaném zabezpečení informací a telematice soukromí dat si můžete od společnosti Webfleet Solutions vyžádat na webové stránce **www.webfleet.com**

Kontaktujte nás:
privacy@webfleet.com

CERTIFIKOVANÉ ZABEZPEČENÍ INFORMACÍ A TELEMATIKA SOUKROMÍ DAT

webfleet solutions

VE SPOLEČNOSTI WEBFLEET SOLUTIONS, **BEREME ZABEZPEČENÍ INFORMACÍ A SOUKROMÍ DAT VELICE VÁŽNĚ.**

Soustavně investujeme do našeho inženýrství, osvědčených technologií, procesů a personálu, abychom mohli vždy poskytnout ty nejspolehlivější platformy telematických služeb na trhu.

VÝHODY PLATFORMY SLUŽBY WEBFLEET SOLUTIONS

CERTIFIKOVANÉ ZABEZPEČENÍ INFORMACÍ PODLE NORMY ISO/IEC 27001:2013
Naše platforma služeb a naše vyspělé postupy byly certifikovány, abychom naším zákazníkům poskytli možnost využívat nejvyšší úroveň ochrany v oblasti zabezpečení informací a soukromí dat.

ŠIFROVÁNÍ EV SSL NEJVYŠŠÍHO STANDARDU
Zabezpečené, šifrované přihlášení a přenos dat na naší platformu služeb. Máte jistotu, že jsou vaše data v bezpečí

LOKÁLNÍ INSTALACE
Národní a mezinárodní instalační partneři

PRVOTŘÍDNÍ PODPORA
Od místních prodejců a integrátorů systému

APP CENTER
Prověřené integrace a rozšiřující aplikace dostupné v centru App Center

Není proto překvapením, že v oblasti správy vozového parku a telematiky patříme ke světové špičce.

Protože patříme mezi největší světové poskytovatele telematických služeb, snažíme se neustále vylepšovat naše služby, abychom měli jistotu, že jsme pro vaši firmu tím nejlepším současným i budoucím partnerem.

Certifikace podle normy ISO 27001

Náš systém správy zabezpečení informací (ISMS) zahrnuje všechny naše zásadní firemní procesy nezbytné k zabezpečení informačních prostředků souvisejících s platformou služby Webfleet Solutions. Zahrnuje architekturu, inženýrství, zajištění kvality a IT služby poskytované společností Webfleet Solutions B.V v našem technologickém ředitelství v Německu i v našich zabezpečených kolokačních datových centrech v rámci Evropské unie. To je ve shodě s normou ISO/IEC 27001:2013 a zavedeno (podrobný popis je uveden v prohlášení o použitelnosti – verze z listopadu 2016).

„Certifikát ISO 27001 zdůrazňuje, že máme plnou kontrolu nad svými procesy, a především, že jsou data našich klientů v bezpečí. To je rozhodující proto, abychom byli schopni poskytovat mimořádně užitečné řešení pro správu vozového parku typu software jako služba (SaaS).“

Thomas Schmidt, generální ředitel, Webfleet Solutions

Systém správy zabezpečení informací

Základním stavebním kamenem závazku společnosti Webfleet Solutions vůči zabezpečení informací jsou naše zásady zabezpečení a programy, které zahrnují organizaci a správu zabezpečení informací. Na základě našeho přísného systému řízení rizik spojeného s našimi firemními cíli je přesně stanovená bezpečnostní zóna provozována v rámci systému ISMS, který zahrnuje mimo jiné i následující témata:

ZÁSADY ZABEZPEČENÍ INFORMACÍ

Detailní zásady zabezpečení jsou navrženy tak, aby vedení poskytly směr a podporu systému správy informací a všech operací souvisejících s provozem platformy služby Webfleet Solutions.

ORGANIZACE ZABEZPEČENÍ INFORMACÍ

Zabezpečení informací se týká každého.
Role a zodpovědnost všech zaměstnanců jsou založeny na zabezpečení informací. Společně se samostatným týmem pro zabezpečení informací zodpovídají za dodržování normy ISO 27001 i za obecné nařízení o ochraně osobních údajů (GDPR) vydané EU a veškeré příslušné místní právní předpisy na ochranu soukromí všichni zaměstnanci.

ZABEZPEČENÍ LIDSKÝCH ZDROJŮ

Zabezpečení informací je klíčové před zahájením pracovního poměru, v jeho průběhu i po jeho skončení. Tento proces zahrnuje výběr správných zaměstnanců a jejich neustálé speciální proškolování.

SPRÁVA POLOŽEK

Skladování, vlastnictví a údržba během životnosti položek zajišťuje správnou kategorizaci, označování a přiřazení vlastníků rizika. Tento proces zahrnuje bezpečné zacházení s duševním vlastnictvím společnosti a daty zákazníků.

ŘÍZENÍ PŘÍSTUPU

Prostřednictvím správy identity vychází veškeré omezení přístupu z toho, co je nutné mít a co je nutné znát. Dodatečné kontroly pomáhají zabránit neoprávněnému přístupu. Například přihlášení do systému a jeho monitorování umožňuje v naší bezpečnostní zóně detekci v reálném čase.

ŠIFROVÁNÍ

Investujeme prostředky do nejmodernějších hardwarových a softwarových řešení. Prověřené šifrovací technologie chrání důvěrnost a integritu dat našich zákazníků i naše operační systémy.

FYZICKÉ A ENVIRONMENTÁLNÍ ZABEZPEČENÍ

Díky našim přísným požadavkům na ochranu osobních údajů provozujeme v rámci Evropské unie dvě nezávislá datová centra úrovně 3+. Naše prověřená konfigurace formou „aktivní/aktivní“ zajišťuje obnovení po havárii a vysoce dostupné funkce, které jsou pravidelně testovány.

ZABEZPEČENÍ PROVOZU

V rámci našeho provozu usilujeme o udržení řízeného, závazného a opakovatelného postupu. Vytvořením standardních hodnot pro zabezpečení jsou úrovně rizika řízeny tak, aby umožnily efektivní provoz.

Hlavní body bezpečnosti provozu:

- **Provozní postupy a dokumentace**
- **Zálohování / obnovení testů důležitých systémů**
- **Monitorování provozních prostředí**
- **Řízení událostí, problémů a změn založené na doporučených postupech**
- **Řízení kapacity včetně zátěžového testování**
- **Rozdělení povinností**
- **Hardening (zabezpečení) systémů**
- **Oddělení prostředí pro vývoj, testování a výrobu**
- **Prověřování ohrožení zabezpečení**
- **Penetrační testování**
- **Řízení oprav**

ZABEZPEČENÍ KOMUNIKACE

Zabezpečení dat „během přepravy“ vyžaduje zabezpečenou síť, která se dá použít pro cestování. Používáme bezpečné způsoby komunikace, například:

- **Rozdělení sítě**
- **Oddělení sítě VLAN, DMZ s víceúrovňovými bránami firewall**
- **Řízení přístupu k síti (NAC)**
- **Standardní šifrování pomocí nejnovějších průmyslových norem**

Let's drive business. Further.

webfleet.com

webfleet solutions