VOLKSWAGEN
FINANCIAL SERVICES
KLÍČ K MOBILITĚ

Prohlášení informační bezpečnosti

Volkswagen Financial Services

Obsah

I. Anotace

Prohlášení managementu: Volkswagen Financial Services bere bezpečnost informací, systémů a aplikací i celé infrastruktury velmi vážně. Z tohoto důvodu jsou vytvořeny politiky, principy a procedury, které zajišťují implementaci a dodržování zásad informační bezpečnosti napříč celou organizací, ale i směrem k partnerům, dodavatelům a klientům.

II. Vymezení

Toto prohlášení informační bezpečnosti Volkswagen Financial Services vzniklo za účelem poskytnutí základního přehledu opatření informační bezpečnosti, které pomáhají chránit informace, osobní údaje, systémy, aplikace i celou infrastrukturu organizace Volkswagen Financial Services. Tento přehled není vyčerpávající a neposkytuje kompletní výčet postupů a opatření ke zmírnění veškerých informačních rizik organizace.

Informace uvedené v tomto prohlášení jsou určeny pro stávající a budoucí klienty Volkswagen Financial Services, zaměstnance, partnery a dodavatele.

III. Organizace informační bezpečnosti

Volkswagen Financial Services si uvědomuje hodnotu informačních aktiv, kterými disponuje, a proto zodpovědně přistupuje k jejich ochraně. Volkswagen Financial Services svou informační bezpečnost staví na přístupu založeném na komplexním řízení rizik a dodržování standardů skupiny Volkswagen Financial Services – IT Minimum Standards, které jsou postaveny na světově uznávaných standardech a metodikách, jako například ISO/IEC 27 001/2, COBIT, ITIL, NIST.

Informační bezpečnost ve Volkswagen Financial Services je zaštítěna manažerem informační bezpečnosti – Chief Information Security Officer (CISO), který vede tým specialistů z oblasti informační bezpečnosti. V úseku informační bezpečnosti je podporovaný neustálý osobní rozvoj a nepřetržité sledování novinek a trendů v oblasti informační bezpečnosti. CISO a členové jeho týmu jsou držiteli nejrůznějších profesionálních certifikátů, například:

CISSP (Certified Information System Security Professional),
CCSP (Certified Cloud Security Professional),
CEH (Certified Ethical Hacker),
CISA (Certified Information Systems Auditor),
ISO 27001 Lead auditor atd.

Všichni zaměstnanci a spolupracovníci Volkswagen Financial Services jsou povinni se řídit po celou dobu spolupráce pravidly politiky informační bezpečnosti Volkswagen Financial Services. Dále všichni pravidelně prochází školením v oblasti pravidel a zásad informační bezpečnosti, což posiluje všeobecné povědomí a přispívá ke komplexnímu zajištění informační bezpečnosti v organizaci.

1. Organizace informační bezpečnosti

1.1 Systém řízení informační bezpečnosti

Volkswagen Financial Services zavedl systém řízení informační bezpečnosti na základě „best practise“ vycházejících z mezinárodně uznávaných standardů a metodik, zejména z ISO/IEC 27001/2 a COBIT. Tyto standardy jsou uvedeny v celoorganizační politice přístupu k informační bezpečnosti.

1.2 IT Architektura

Bezpečná a stabilní IT architektura je pro fungování organizace stěžejní. Pro zajištění bezpečné IT Architektury jsou ve Volkswagen Financial Services definovány zásady, které odpovídají obecně uznávaným postupům. Řídíme a udržujeme aktuální technologické i aplikační portfolio. Toto vše přispívá k usnadňování plánování a rozhodování budoucího vývoje IT i ke zkvalitnění procesů nákupu a zefektivnění komunikace jak s dodavateli, tak i uvnitř organizace.

1.3 Fyzická bezpečnost

V uživatelské bezpečnostní politice Volkswagen Financial Services pozornost věnujeme i vhodnému nastavení fyzické bezpečnosti a pravidel pro její udržení. Jsou definovány jak zásady pro fyzickou ochranu informačních aktiv, tak i pro ochranu fyzického perimetru organizace a jejího vybavení.

2. Bezpečnost lidských zdrojů

2.1 Personální bezpečnost

Personální bezpečnost považujeme za klíčovou součást informační bezpečnosti. Proto ji řídíme hned od samého počátku zahajování pracovních, dodavatelských či obdobných vztahů. Každá spolupráce je mimo jiné založena dohodou o informační bezpečnosti, ve které se spolupracující osoby zavazují k dodržování nejdůležitějších zásad a pravidel. Tato pravidla platí i pro externí spolupracovníky.

Během spolupráce prochází jak zaměstnanci, tak i další spolupracovníci pravidelným e-learningovým školením, které reflektuje aktuální hrozby, zranitelnosti a trendy v informační bezpečnosti. Pro změny nebo ukončování pracovních, dodavatelských či obdobných vztahů máme vypracované procesy, které berou na zřetel informační požadavky a jsou nastavené tak, aby snižovaly související rizika.

2.2 Vztahy s dodavateli a třetími stranami

V prostředí Volkswagen Financial Services rozdělujeme dodavatele a třetí strany do několika typů a pro každý typ máme vybudované speciální postupy a procedury. Prvním typem je outsourcing externích spolupracovníků, kteří se při zahájení spolupráce zavazují k dodržování základních principů a pravidel informační bezpečnosti. Druhým typem jsou dodavatelé služeb a produktů, přičemž pro tyto dodavatele platí pravidla informační bezpečnosti uvedená v nákupních podmínkách Volkswagen Financial Services. Dodavatele zároveň hodnotíme z hlediska rizikovosti předmětu plnění a tam, kde je identifikována vysoká míra rizika, uzavíráme s dodavatelem speciální smlouvu upravující další požadavky informační bezpečnosti. Třetím typem jsou obchodní partneři, se kterými uzavíráme speciální smluvní ujednání.

2.3 Řízení identit a přístupových práv

Volkswagen Financial Services má vytvořenu závaznou politiku pro řízení přístupů, která respektuje všechny základní principy informační bezpečnosti – zejména princip nejnižších privilegií, oddělení odpovědností a principy potřeby vědět a potřeby sdílet. Pozornost zaměřujeme i na zajištění vyhnutí se konfliktu rolí a odpovědností. Řízení privilegovaných účtů a přístupů je pokryto definovaným procesem a podporováno specializovaným nástrojem pro řízení privilegovaných účtů. Napříč všemi systémy a aplikacemi vynucujeme politiku pro řízení bezpečnosti hesel. Důsledně dodržujeme jedinečnost a adresnost přidělovaných přístupů pro zachování autenticity, nepopiratelnosti a umožnění auditovatelnosti. Využíváme vícefaktorovou autentizaci.

2.4 Ochrana osobních údajů

Svých klientů, partnerů i spolupracovníků si velmi vážíme, a proto chráníme veškeré osobní údaje, které nám svěří. Důsledně dodržujeme účelnost zpracovávaných osobních údajů a dbáme na zavádění opatření ke zvýšení jejich ochrany. Používáme anonymizaci osobních údajů, šifrujeme a pečlivě kontrolujeme nakládání s osobními údaji v rámci interních procesů.

3. Stabilita, růst a udržitelnost organizace

3.1 Řízení IT a informačních rizik

Ve Volkswagen Financial Services pozornost směřujeme také k řízení IT a informačních rizik. Identifikujeme zranitelnosti, modelujeme hrozby a pravidelně vyhodnocujeme pravděpodobnosti a dopady definovaných rizik. Přijímáme opatření k nápravě či zmírnění situace a efektivitu zavedených opatření následně monitorujeme. Pro každý systém či aplikaci je nastavena specifická úroveň ochrany, která odpovídá významnosti procesu, jež je daným systémem či aplikací podporován.

3.2 Řízení incidentů informační bezpečnosti

Máme zavedeny mechanismy pro detekci, identifikaci, řízení a analýzu událostí informační bezpečnosti. Pro včasné zachycení a zmírnění dopadů jsou nastaveny procesy s odpovídajícími reakčními dobami tak, aby bylo možné předejít šíření či zhoršení dopadů incidentu. Pro zajištění efektivní spolupráce při identifikaci a řešení incidentů, ale také z důvodu zvyšování povědomí o této problematice, prochází všichni zaměstnanci a spolupracovníci speciálním školením.

3.3 Zachování kontinuity IT služeb

Veškeré IT služby mají nastavenu konkrétní úroveň kritičnosti, abychom efektivně mohli řídit kontinuitu provozu. Data pravidelně zálohujeme, přičemž frekvence a retence záloh odpovídá definované citlivosti dat. Jsou nastaveny plány a postupy obnovy pro jednotlivé aplikace a systémy, včetně stanovení maximální doby a bodu obnovy.

3.4 Compliance

Včasně a zodpovědně reagujeme na potřebu shody s regulacemi, legislativou, interními i mezinárodními standardy. Za pravidelný monitoring shody je odpovědné právní oddělení, které v této oblasti úzce spolupracuje s ostatními součástmi organizace. Na ochranu osobních údajů dohlíží jmenovaný Pověřenec pro ochranu osobních údajů. Pro zajištění shody s interními předpisy je zaveden kontrolní systém, jehož součástí je definice jak pravidelných, tak ad hoc kontrol. Významnou součástí jsou i pravidelné audity, které vyhodnocují aktuální stav shody Volkswagen Financial Services s legislativou a dalšími požadavky.

4. Informační aktiva

4.1 Řízení informačních aktiv

Za informační aktivum ve Volkswagen Financial Services považujeme hardware, software, data a informace mající hodnotu (důležitost) pro organizaci. Informační aktiva mohou rovněž zahrnovat méně zřejmé položky, například znalosti. Tato aktiva identifikujeme napříč celou společností a hodnotíme je z pohledu jejich důležitosti. Pravidelně zjišťujeme zranitelnosti těchto aktiv i hrozby, které se k nim váží, a identifikujeme tak rizika. Na rizika aktiv reagujeme implementací vhodných bezpečnostních opatření. Veškeré informace ve Volkswagen Financial Services klasifikujeme podle jejich citlivosti a dle přiděleného klasifikačního označení definujeme možné způsoby nakládání s těmito informacemi.

4.2 Akvizice a údržba systémů

Dodavatele našich systémů před navázáním dodavatelského vztahu důkladně prověřujeme a v průběhu spolupráce pravidelně monitorujeme možná související rizika. Nedílnou součástí je vyžadování a udržování principů „security by design“ a „security by default“ v průběhu celého životního cyklu systému. V informačních systémech jsou nastaveny a pravidelně aktualizovány bezpečnostní mechanismy pro zajištění důvěrnosti, integrity a dostupnosti dat zpracovávaných systémy.

4.3 Proces bezpečného vývoje softwaru

Proces vývoje softwaru řídíme s ohledem na dodržování bezpečnostních zásad. Vývoj je realizován výhradně prostřednictvím legálního softwaru na základě předem zajištěných autorských a licenčních ujednání. Využíváme vývojové prostředí oddělené od prostředí produkčního s využitím testovacích dat, která vytváříme specificky pro účely testování, nebo je zcela anonymizujeme. Pozornost směřujeme k důkladnému testování také z pohledu bezpečnosti. Data vstupující do informačních systémů podrobujeme vstupní kontrole správnosti. Systémy a aplikace jsou pravidelně zabezpečovány proti známým zranitelnostem. V průběhu celého životního cyklu softwaru klademe důraz na definování, monitorování a kontrolu implementace bezpečnostních požadavků.

5. Bezpečnost provozu

5.1 Provozní bezpečnost

V oblasti provozní bezpečnosti se řídíme definovanými politikami, procesy a postupy, které pokrývají bezpečnost serverů, klientských stanic, řízení konfigurací, řízení incidentů, problémů i změnové řízení.

5.2 Bezpečnostní monitoring

Máme zaveden systém provozně-bezpečnostního monitoringu. Pravidelně provádíme analýzy systémových a bezpečnostních logů a hodnotíme výstupy z provozu infrastruktury na základě definovaných scénářů.

5.3 Bezpečnost komunikačních kanálů

Bezpečnost na úrovni komunikace zajišťujeme nastavením bezpečnostních zásad ve všech typech komunikačních kanálů. Máme zabudovány bezpečnostní a monitorovací prvky, které slouží k včasné detekci, zamezení narušení bezpečnosti a předcházejí selhání infrastruktury. Součástí interních politik pro řízení bezpečnosti jsou i zásady a postupy pro bezpečný přenos informací jak uvnitř organizace, tak i pro přenos mimo organizaci.

5.4 Kryptografie

Pro zajištění bezpečnosti statických dat v úložištích i dat při přenosech a zpracování sledujeme nejnovější trendy a používáme definované a schválené kryptografické metody a protokoly, které jsou obecně uznávány jako bezpečné.

VOLKSWAGEN FINANCIAL SERVICES
Evropská 866/63 | 160 00 Praha 6
T +420 224 992 410
E klient@vwfs.cz
W vwfs.cz

#mojemobilita