Bezpečnost IT

Obsah:

1. Účel

Pravidla bezpečnosti IT (informační technologie) popsaná v této organizační normě definují zásadní cíle, strategii a odpovědnosti k zajištění bezpečnosti IT ve společnosti Škoda Auto (dále společnost). Jsou definována na základě ČSN ISO 27001:2005 a dalších mezinárodních předpisů a standardů (viz kap. 6), a směřují k jejich zakotvení ve společnosti.
Tato norma navazuje na Bezpečnostní politiku IT VW a související předpisy koncernu VW.
Zajištění bezpečnosti IT zahrnuje zajištění technické infrastruktury, kontrolu a řízení informačního toku. Pravidla bezpečnosti slouží k ochraně důvěrnosti, integrity a dostupnosti informací, jakož i k zachování práv a zájmů společnosti a všech fyzických a právnických osob, které jsou se společností v obchodním styku nebo pro ni pracují.

Pro vytvoření a udržení důvěry v bezpečnost IT jsou ve společnosti vytvořeny a realizovány předpisy pro ochranu informací, které:

- zvyšují povědomí o možnostech a nebezpečích v oblasti IT, o důvodech a nutnosti ochrany informací
- zavádějí bezpečnost IT jako standard v procesech společnosti

2. Oblast působnosti

Tato organizační norma je závazná pro všechny:

- vedoucí OJ společnosti a jimi určené zaměstnance
- uživatele IT (interní a externí)
- dceřiné společnosti

3. Základní pojmy/zkratky

IT	Informační technologie (jsou tvořeny IS a ICT)
IS	Informační systémy
ICT	Informační a komunikační technologie
Komunikační zařízení	Osobní počítač, pracovní stanice, notebook, PDA (Personal Digital Assistant), MDA (Mobile Digital Assistant), mobilní telefon
SW / Software	Sada všech počítačových programů umístěných v komunikačním zařízení
Škodlivý SW	Nebezpečný SW jako jsou viry a jiný škodlivý kód
HW / Hardware	Veškeré fyzicky existující technické vybavení komunikačního zařízení
Oprávněná osoba	Uživatel IT s oprávněním pro čtení nebo změnu konkrétní informace a dále uživatel IT s oprávněním pro používání určitého HW.
Uživatel IT	Každá fyzická osoba, požadující a využívající přístup k IT nebo na nich uložených informací společnosti
Vlastník dat	Vedoucí OJ, kde data vznikají, pořizují se prvně do IS, nebo kde se daná data jako v jediném útvaru společnosti zpracovávají nebo využívají

Informace	Aktiva mající pro společnost hodnotu, přičemž mohou existovat v různých formách (tištěná, elektronická a jiné)
Důvěrnost	Zpřístupnění/sdělení informace pouze oprávněné osobě
Dostupnost	Přístupnost informace pro oprávněného uživatele v okamžiku její potřeby
Integrita	Zajištění pravdivosti (správnosti) a úplnosti informace
Autentizace	Ověření identifikace při přístupu k informacím
Autorizace	Umožnění přístupu k informacím pouze oprávněným osobám a pouze v rozsahu nezbytně nutném pro plnění pracovních úkolů
Auditování	Zaznamenávání a kontrola přístupu k informaci
Prokazatelnost	Nepopiratelnost přístupu k informaci a jejímu zpracování
CISO (Chief Information Security Officer)	Zmocněnec pro bezpečnost IT – vedoucí EOS, řídí bezpečnost IT ve společnosti
ISSO (Information Systems Security Organisation)	Globální organizace bezpečnosti IT koncernu Volkswagen
Pověřenec pro ochranu dat	Navrhuje opatření směřující ke zvýšení bezpečnosti dat, dbá o jednotný stav znalostí v otázkách bezpečnosti dat ve společnosti. Na základě vyhodnocení rizik vytváří standardy bezpečnosti dat. Ve spolupráci s ostatními útvary řeší incidenty v oblasti bezpečnosti dat.
Příslušný správce technologického HW	OJ, v jejíž kompetenci je správa technologického HW (např. v oblasti V - útvary údržby, v oblasti T - TM/2)
EOx	Organizační jednotky (OJ) spadající pod EO, které jsou odpovědné za správu a vývoj IT ve společnosti
ServiceDesk	Centrální místo pro podporu IT uživatelů
Bezpečnostní standardy IT	Systémová, procesní a organizační dokumentace týkající se bezpečnosti IT
MFA2 karta	Multifunkční zaměstnanecký průkaz

4. Kompetence

Činnost	Odpovědnost
Společně stanovují obecné zásady bezpečnosti informací.	ZO, EOS Pověřenec pro ochranu dat
Seznamuje zaměstnance s procesní a organizační dokumentací, standardy v oblasti bezpečnosti IT a s významem jejich dodržování. Ve své oblasti působnosti odpovídá za to, že při zacházení s informacemi a IT je vždy zajištěna přiměřená bezpečnost IT. Zajišťuje uplatňování pravidel bezpečnosti IT a průběžně kontroluje dodržování předpisů. V zájmu omezení bezpečnostních rizik je povinen zajistit vzdělávání zaměstnanců v oblasti bezpečnosti IT.	Vedoucí OJ
V oblasti bezpečnosti IT - zjišťuje rizika, vytváří standardy a pravidla a metodicky řídí jejich praktickou aplikaci, provádí analýzy a audity, plánuje a kontroluje provedení efektivních opatření a ve spolupráci s ostatními útvary řeší incidenty bezpečnosti IT. Podporuje vedoucí zaměstnance při vytváření povědomí o významu bezpečnosti IT, stará se o jednotný stav znalostí v otázkách bezpečnosti IT ve společnosti. Schvaluje výjimky z ustanovení této organizační normy. Zpracovává podklady pro nástupní školení nových zaměstnanců společnosti (v oblasti bezpečnosti IT)	EOS
Provádí změny v HW (např. instalace/odebrání pevných disků, disketových mechanik, paměťových modulů) a změn SW a jeho nastavení. Zajišťuje připojení komunikačních zařízení do datové sítě společnosti. Zajišťuje opravu a likvidaci komunikačních zařízení.	EOI
Provádí správu a změny technologického HW a SW (např. instalace/odebrání pevných disků, disketových mechanik, paměťových modulů) a změn SW a jeho nastavení. Zajišťuje opravu a likvidaci technologického HW a SW.	příslušný správce technologického HW

Spolupracuje s EOS na tvorbě standardů bezpečnosti IT, aktivně je realizuje a systémově vynucuje jejich dodržování uživateli. Odpovídá za zajištění standardů bezpečnosti, plánuje nákup a provoz IT v souladu s bezpečnostními standardy IT. Přijímá opatření k zabezpečení toho, aby přístupy k informacím byly jednoznačně identifikovatelné, rekonstruovatelné a nepopiratelné. Dbá na to, aby pouze jednoznačně identifikované osoby s příslušným oprávněním mohly obdržet přístup k informacím chráněným odpovídajícím způsobem.	EOx
Koordinuje bezpečnost IT v rámci koncernu VW a prosazuje zavádění jednotných pravidel a standardů.	ISSO (IS Security Organisation)
Koordinuje bezpečnost IT v rámci společnosti a prosazuje zavádění jednotných pravidel a standardů.	CISO (Chief Information Security Officer)

VŽDY	NIKDY	
Odpovídá za řádné využívání svěřeného HW, SW a informací výhradně pro potřeby společnosti a v rámci plnění pracovních úkolů.	Nešíří uvnitř společnosti a ze společnosti informace s nepracovním obsahem (např. řetězové e-maily, vtipy).	Uživatel IT
Používá SW a data ve vlastnictví společnosti pouze na IT společnosti.	Nepoužívá a neukládá SW, který není ve vlastnictví společnosti na IT společnosti, a to ani k pracovním účelům (např. freeware, shareware).	
V rámci stanovených úkolů je odpovědný za označení příslušného stupně důvěrnosti informací ihned po jejich vytvoření a za jejich bezpečnost v případě jejich použití.	Nepoužívá pro svou práci cizí uživatelský účet. Nikomu nesděluje svůj uživatelský účet a heslo/a.	
Nakládá přiměřeně s poskytnutými IT a informacemi, chrání je před ztrátou, poškozením, nebo neoprávněným použitím či změnou, resp. zfalšováním. Dodržuje pokyny výrobce a zásady bezpečnosti a ochrany zdraví při práci.	Nepoužívá ke své práci soukromý HW (včetně příslušenství a nosičů dat), ani jej nepřipojuje k IT společnosti (např. připojování soukromé USB paměti k pracovnímu PC, připojování soukromého mobilního telefonu pomocí Bluetooth ke komunikačnímu zařízení společnosti).	
Hlásí svému nadřízenému nebo EOS/2 porušení, nebo podezření z porušení předpisů týkajících se bezpečnosti IT nebo slabiny bezpečnosti IT v systémech, jednotlivých funkcích a funkční poruchy relevantní pro bezpečnost IT.	Nezasahuje do konfigurace HW ani nastavení SW na komunikačních zařízeních společnosti (např. výměna paměti RAM, vypínání běžících služeb, změna konfigurace IE).	
Při používání IT dodržuje opatření k ochraně důvěrnosti, dostupnosti, integrity a prokazatelnosti.	Neposkytuje data sdílením z přiděleného komunikačního zařízení dalším uživatelům/komunikačním zařízením zapojeným do datové sítě společnosti.	
Dodržuje procesní a organizační dokumentaci a standardy v oblasti bezpečnosti IT, které se ho prokazatelně týkají.		
Jednou ročně absolvuje školení v oblasti bezpečnosti IT.		

5. Postup

Informace a zařízení poskytnutá ke zpracování informací a ke komunikaci jsou cenným majetkem společnosti, který podléhá ochraně. Předávání informací a programů ve vlastnictví společnosti externím organizacím (např. externím osobám ve společných projektech) je přípustné zásadně pouze v rámci písemně dohodnutého zadání úkolu a s písemným souhlasem vlastníka dat.

Principy pravidel bezpečnosti IT

- Každý, kdo využívá informace, je v rámci stanovených úkolů odpovědný za jejich zabezpečení.
- Všechny informace musí být ihned po vytvoření odpovídajícím způsobem klasifikovány a odpovídajícím způsobem zabezpečeny.
- Pouze jednoznačně identifikované osoby s příslušným oprávněním mohou

obdržet přístup k informacím chráněným odpovídajícím způsobem.
- Všechny přístupy k informacím musí být jednoznačně identifikovatelné, rekonstruovatelné a prokazatelné.

Přestupky

Za přestupek proti bezpečnosti IT je považováno úmyslné nebo nedbalostní jednání, které zejména:
- poškozuje dobré jméno společnosti
- ohrožuje bezpečnost zaměstnanců, smluvních partnerů nebo majetku společnosti
- způsobuje společnosti skutečnou nebo potenciální finanční ztrátu
- umožňuje neoprávněný přístup k informacím, jejich neoprávněné poskytnutí nebo neoprávněnou modifikaci
- zahrnuje využití podnikových informací pro nezákonné účely.

Přestupky proti předpisům bezpečnosti IT jsou posuzovány individuálně podle příslušných zákonných, smluvních a provozních ustanovení v jejich platném znění a jsou sankcionovány v souladu s příslušnými obecně závaznými právními předpisy.

Připojení komunikačních zařízení do datové sítě společnosti

Připojit komunikační zařízení do datové sítě společnosti je povoleno pouze tehdy, pokud je zařízení ve vlastnictví společnosti nebo společnosti, ve které má společnost Škoda Auto nebo jedna ze společností koncernu Volkswagen většinový podíl. Připojení smí provést / nastavit pouze EOI.

Zabezpečení IT před ztrátou, poškozením a krádeží

S IT společnosti je nutné nakládat přiměřeně a chránit je před ztrátou, poškozením nebo krádeží. Komunikační zařízení nesmí zůstat volně přístupné a bez dohledu.
- Přeprava komunikačních přístrojů mimo hranice společnosti je možná pouze s písemným souhlasem ZO (s výjimkou mobilních telefonů).
- Přenosné komunikační zařízení nesmí být bez dohledu uloženo v motorovém vozidle.
- Při cestách letadlem a vlakem musí být přenosné komunikační zařízení zásadně přepravováno jako příruční zavazadlo.

Zabezpečení IT před neoprávněným využitím

Ke komunikačním zařízením společnosti smí mít přístup pouze oprávněné osoby. Neoprávněné osoby (platí i pro členy rodiny, přátele atd.) nesmí mít možnost použít zařízení nebo nahlédnout na informace klasifikované stupněm interní, důvěrné nebo tajné (viz OS – 161/3 - Zachování tajemství).
Jestliže je na komunikačním zařízení spuštěno dlouhotrvající zpracování, které se nesmí přerušit nebo se potřebuje uživatel na nutnou dobu od zařízení vzdálit (např. přestávka, jednání, toaleta) musí uživatel komunikační zařízení zabezpečit proti neoprávněnému využití spořičem obrazovky chráněným heslem, nebo obdobně fungujícím mechanismem. Uživatelé, kteří používají k přihlašování do systému MFA2 kartu, musí při každém fyzickém opuštění komunikačního zařízení vyjmout MFA2 kartu ze čtečky. Po ukončení práce s komunikačním zařízením je uživatel povinen provést řádné ukončení systému a vypnout přístroj včetně obrazovky a všech přímo napojených komunikačních přístrojů.

Zabezpečení koncových zařízení před škodlivými programy (antivir a bezpečnostní aktualizace SW)

Pravidla ochrany před viry a škodlivými programy stanovuje MP Antivirová ochrana.
Komunikační přístroje, systémy a nosiče dat musí být pravidelně a při podezření na výskyt škodlivého SW okamžitě kontrolovány pomocí aktualizovaného antivirového SW (na kancelářských PC je to zajištěno antivirovým programem automaticky).
V případě podezření na napadení škodlivým SW nebo nefunkčnosti antivirového programu nesmí být komunikační přístroj nadále používán a musí být informován ServiceDesk (resp. příslušný správce technologického HW), který zajistí odstranění škodlivého SW.
Bezpečnostní aktualizace jsou na kancelářské PC instalovány automaticky a

	uživatel je o jejich instalaci informován.
Bezpečnost elektronické pošty/internetu	Elektronická pošta musí být automaticky prověřována na přítomnost nevyžádaných zpráv (tzv. spam). Tato nevyžádaná pošta musí být automaticky mazána. Pokud přesto uživatel ve své schránce nalezne nevyžádanou poštu, měl by ji bez otevření smazat. Vytváření, odesílání a přeposílání řetězových a hromadných nevyžádaných obchodních a soukromých sdělení je zakázáno. Elektronická pošta není určena k předávání objemných souborů. Odesílatel je jako původce elektronické zprávy odpovědný za obsah a rozdělovník, příjemce je odpovědný za další zpracování a distribuci elektronické zprávy. Elektronické zprávy a jejich přílohy musí být před prvním spuštěním zkontrolovány aktuálním antivirovým softwarem na výskyt nebezpečného softwaru (na kancelářských PC je zajištěno antivirovým programem automaticky). Internet je možné používat pouze pro pracovní účely. Bližší specifikace a pravidla užívání viz OP 123/2 – Internet – přidělení a užívání.
Zálohování	Informace smí být ukládány výhradně na k tomu určených síťových discích, kde je zajištěno jejich centrální a automatické zálohování. Ukládání informací na lokální disk komunikačního zařízení je možné pouze pro dočasnou pracovní potřebu. Úložištěm na netechnologických PC s operačním systémem Windows smí být výhradně složka Dokumenty (tzv. uživatelský profil daného uživatele), nebo její podsložky. Uživatel je odpovědný za zálohování těch dat, která jsou uložena na lokálních datových nosičích (pevné disky komunikačních zařízení, CD, DVD a další) a jejich případnou ztrátu. Datové nosiče, které obsahují důvěrná nebo tajná data musí být označeny odpovídajícím způsobem, katalogizovány, a uloženy v zamčeném prostoru (skříň, zásuvka).
Přístup uživatele k informacím	Uživatel smí získat přístup (kromě veřejných informací) pouze k těm informacím, které potřebuje v rámci plnění pracovního úkolu. Větší rozsah musí prokazatelně schválit vlastník dat Uživatelský účet nebo přístupové oprávnění, které již není zapotřebí, musí uživatel nahlásit příslušnému zřizovateli přístupu, který je povinen ho vymazat. Nepotřebná médie a pro identifikaci (např. MFA2 karty, SecureID tokeny) musí být bezodkladně navráceny vydavateli, nebo pověřenému útvaru. Přístup k informacím, práci s nimi a jejich ukládání na síťové disky upravuje MP EOI Práce s daty v síti.
Evidence komunikačních zařízení	Každé komunikační zařízení ve vlastnictví nebo používání společnosti musí být evidováno v centrální evidenci IT (blíže viz MP Evidence IT).

6. Související podklady

Zákon č.140/1961 Sb., trestní zákon
Zákon č.101/2000 Sb., zákon o ochraně osobních údajů
Zákon č.148/1998 Sb., zákon o ochraně utajovaných skutečností
ČSN ISO/IEC 27001:2005
ISO/IEC 9001:2000
Bezpečnostní politika IS VW a související předpisy koncernu VW
Politika společnosti Škoda Auto
Příručka integrovaného systému řízení Škoda Auto
OS 122/4 Ochrana a zabezpečení dat

ON.1.019 Přístupová práva do informačních systémů
OP 123/2 Internet – Přidělení a užívání
OS 161/3 Zachování tajemství
OS 162/2 Ochranná opatření
OS 162/3 Ochrana majetku
Pracovní řád
Intranet EO:
- MP Práce s daty v síti
- MP Antivirová ochrana
- MP Evidence IT

Intranet EOS:
- Uživatelský účet a přístup uživatele k informacím – stanovování hesel a PINů

7. Dokumentace

Formulář Oprávnění k přenosu předmětů mimo areál závodu

8. Přílohy

neobsazeno

Holger Kintscher
E/ Oblast ekonomie

Andreas Hafemann
EO/ Informační systémy a organizace