Směrnice

o bezpečnosti informací

Informace k dokumentu	
Název	IS1-4 IA Směrnice o bezpečnosti informací
Zkratka dokumentu / reference:	IS1-4
Zhotoveno:	09.11.2016
Poslední úprava:	14. 8. 2024
Počet stran:	7
Stupeň důvěrnosti	veřejné
Číslo verze:	2
Stav zpracování:	Uvolněno
Nutné uvolnit:	ano
Uvolněno dne:	14.08.2024
Uvolněno kým: Vedení společnosti / ISB	Schválení prostřednictvím prokazatelného schválení platné hlavní verze na intranetové stránce oddělení IS ze strany pověřence pro bezpečnost informací a vedení společnosti
Ustanovení vstoupí v platnost:	1. 9. 2024
Majitel dokumentu:	ISB
Oblast platnosti:	Celá skupina IDEAL Automotive po celém světě (IA)

Obsah

1. Význam zpracování informací 3
2. Zastřešující cíle 3
2.1 Detailní cíle 3
3. Řízení bezpečnosti informací 4
4. Bezpečnostní opatření 5
5. Zlepšení bezpečnosti 6
6. Důsledky nedodržení 6
7. Odkaz na Prohlášení o zásadách IA 6
8. Postup v případě změn 7
9. Oblast platnosti 7

Vedení společnosti tímto přijímá jako součást své strategie následující směrnici o bezpečnosti informací:

1. Význam zpracování informací

Zpracování informací hraje klíčovou roli v našich obchodních operacích. Veškeré podstatné strategické a operativní funkce a úkoly jsou významně podporovány informačními a komunikačními technologiemi (Information and Communication Technology „ICT“). Výpadek systémů ICT musí být možné v krátké době kompenzovat. Naše podnikání se nesmí zhroutit ani v dílčích oblastech. Protože naše hlavní kompetence spočívá v partnerském vývoji inovativních produktů ve spolupráci se zákazníky a dodavateli, je ochrana těchto informací před neoprávněným přístupem a neoprávněnými změnami životně důležitá.

2. Zastřešující cíle

Dostupnost našich dat a ICT systémů ve všech technologicky závislých a obchodních oblastech je zajištěna tak, aby bylo možné tolerovat očekávané prostoje. Poruchy a nesrovnalosti v datech a systémech ICT jsou přijatelné pouze v omezené míře a pouze ve výjimečných případech (integrita). Požadavky na důvěrnost mají běžnou úroveň, která je orientována na soulad s právními předpisy. Informace, které jsou klasifikovány jako důvěrné nebo tajné z důvodu interní klasifikace či smluvních specifikací našich zákazníků, musí být obzvláště chráněny.

Standardní bezpečnostní opatření musí být ekonomicky odůvodnitelná ve vztahu k hodnotě informací vyžadujících ochranu a systémům ICT. Je třeba zamezit škodám s vysokými finančními dopady.

Všichni zaměstnanci společnosti dodržují příslušnou legislativu (např. zákony a předpisy o ochraně dat), interní procesní a metodické pokyny a příslušné smluvní předpisy. Je třeba se vyhnout negativním finančním a nehmotným důsledkům pro společnost a zaměstnance v důsledku porušení zákona a porušení smlouvy.

Všichni zaměstnanci a vedení společnosti si uvědomují svou odpovědnost při práci s ICT systémy a podporují bezpečnostní strategii, jak nejlépe dovedou.

2.1 Detailní cíle

Pozdní nebo nesprávná manažerská rozhodnutí mohou mít dalekosáhlé důsledky. Proto je pro management při důležitých rozhodnutích důležitý přístup k aktuálním řídicím datům. U těchto informací musí být zajištěna vysoká úroveň zabezpečení z hlediska dostupnosti a integrity.

Zákony o ochraně údajů a zájmy našich zaměstnanců vyžadují zajištění důvěrnosti údajů zaměstnanců. Osobní údaje našich zaměstnanců proto podléhají vysoké úrovni ochrany důvěrných informací. Totéž platí pro osobní údaje našich obchodních partnerů.

Údaje o poptávkách a nabídkách od našich zákazníků a pro ně, jakož i údaje o konstrukci od našich zákazníků a našeho vývojového oddělení mají velmi vysoké požadavky na důvěrnost. Jejich ztráta nebo krádež může mít za následek konkurenční nevýhody či nároky na náhradu škody vůči nám. Technická a organizační opatření a vysoká pozornost zaměstnanců chrání důvěrnost a zabraňují manipulaci.

Pro logistické oblasti a výrobní závody je zajištěna dostupnost a bezchybnost systémů. Prostoje jsou přijatelné jen ve velmi omezené míře, protože mohou přímo i nepřímo vést ke snížení výnosů a mít negativní dopad na spokojenost zákazníků.

Využití internetu a portálových aplikací k získávání informací a komunikaci je pro nás samozřejmostí. E-mail slouží jako náhrada nebo doplněk jiných komunikačních kanálů. Vhodná opatření zajistí, aby rizika použití zůstala co nejnižší.

3. Řízení bezpečnosti informací

K dosažení cílů bezpečnosti informací byla zřízena bezpečnostní organizace. Byl jmenován pověřenec pro bezpečnost informací (ISB/CISO). Ve své funkci je pověřenec pro bezpečnost informací podřízen přímo vedení společnosti.

Vedení společnosti poskytne pověřenci pro bezpečnost informací dostatečné finanční a časové zdroje, aby mohl být pravidelně školen a informován a dosahoval managementem stanovených cílů bezpečnosti informací.

Správci bezpečnosti ICT a pověřenec pro bezpečnost informací musí být při své práci podporováni uživateli ICT.

Pověřenec pro bezpečnost informací musí být zapojen do všech projektů zavčas, aby ve fázi plánování zohlednil aspekty související s bezpečností. Pokud jsou dotčeny osobní údaje, platí totéž pro pověřence pro ochranu osobních údajů.

Uživatelé ICT se musí řídit pokyny pověřence pro bezpečnost informací v otázkách souvisejících s bezpečností.

4. Bezpečnostní opatření

Pro všechny postupy, informace, ICT aplikace a ICT systémy je jmenována odpovědná osoba, která ve spolupráci s pověřencem pro bezpečnost informací určuje příslušnou potřebnou ochranu.

Pro všechny odpovědné funkce musí být zřízeni zástupci. Prostřednictvím poučení a dostatečné dokumentace musí být zajištěno, aby zástupci mohli plnit své úkoly.

Budovy a prostory jsou chráněny odpovídajícími kontrolami přístupu. Přístup do ICT systémů je chráněn přiměřenými kontrolami přístupu a přístup k datům je chráněn konceptem restriktivního oprávnění.

Na všech ICT systémech se používají programy na ochranu před počítačovými viry. Veškerý přístup na internet je zabezpečen vhodnými firewallovými systémy. Veškeré ochranné programy jsou konfigurovány a spravovány tak, aby poskytovaly účinnou ochranu a zabraňovaly manipulaci. Kromě toho uživatelé ICT podporují tato bezpečnostní opatření bezpečným způsobem práce a informují příslušná místa, jestliže se vyskytnou nějaké abnormality.

Se všemi ICT systémy, aplikacemi a veškerými informacemi je třeba zacházet prostřednictvím vhodných technických a organizačních opatření tak, aby bylo vždy možné dosáhnout cílů ochrany. Technická a organizační opatření musí být pravidelně kontrolována a v případě potřeby upravena.

Ztrátu dat nelze nikdy zcela vyloučit. Rozsáhlé zálohování dat proto zajišťuje, že provoz ICT bude moci být obnoven v krátké době, pokud se části provozních dat ztratí nebo jsou zjevně chybné. Informace jsou jednotně označeny a uloženy tak, aby je bylo možné rychle najít.

Aby se omezily větší škody nebo se jim předešlo v důsledku mimořádných událostí, je třeba na bezpečnostní incidenty reagovat rychle a důsledně. Krizová opatření jsou sestavena do samostatné koncepce havarijní připravenosti. Naším cílem je udržet kritické obchodní procesy i v případě výpadku systému a obnovit dostupnost poruchových systémů v přijatelném časovém období.

Jestliže jsou služby ICT zadávány externím subjektům, specifikujeme konkrétní bezpečnostní požadavky ve smlouvách o úrovni služeb. Pokud je potřeba zpřístupnit dodavatelům údaje s vysokou úrovní ochrany za účelem plnění smlouvy, uložíme jim samostatnou a výslovnou povinnost zachovávat mlčenlivost. Zakládá se právo na kontrolu.

Uživatelé ICT se účastní školení o správném používání služeb ICT a souvisejících bezpečnostních opatřeních. Vedení společnosti podporuje různé formy vzdělávání podle potřeb.

5. Zlepšení bezpečnosti

Systém managementu bezpečnosti informací je pravidelně kontrolován s ohledem na aktuálnost a účinnost. Kromě toho jsou opatření pravidelně kontrolována, zda jsou příslušným zaměstnancům známa, zda je lze implementovat a integrovat do provozního procesu.

Vedení společnosti podporuje neustálé zlepšování úrovně zabezpečení. Zaměstnanci jsou vyzýváni, aby případná zlepšení či slabá místa předávali příslušným místům.

Požadovaná úroveň bezpečnosti a ochrany dat je zajištěna neustálou revizí předpisů a jejich dodržováním. Odchylky jsou analyzovány s cílem zlepšit bezpečnostní situaci a neustále ji udržovat v aktuálním stavu s nejnovějšími ICT bezpečnostními technologiemi.

6. Důsledky nedodržení

Nedodržení ustanovení této směrnice může mít pro společnost závažné důsledky. Porušení tohoto ustanovení může mít, v závislosti na závažnosti a okolnostech, za následek disciplinární či právní důsledky.

7. Odkaz na Prohlášení o zásadách IA

Této směrnici je nadřazeno Prohlášení o zásadách společnosti IDEAL Automotive, které je pravidelně revidováno a v případě potřeby aktualizováno. Všichni zaměstnanci jsou povinni se informovat o aktuálním obsahu Prohlášení o zásadách a zajistit, aby jejich jednání bylo v souladu se zde uvedenými zásadami.

s.frey@ideal-automotive.com, Nov 11,2024 08:11:01 AM UTC

8. Postup v případě změn

Změny směrnic o bezpečnosti informací jsou prováděny systematicky a transparentně. Každou plánovanou změnu nejprve ověří a schválí management bezpečnosti informací. Nový nebo změněný obsah bude začleněn do našeho školícího programu, abychom zajistili pochopení a implementaci specifikací.

9. Oblast platnosti

Tato směrnice se vztahuje na všechny zaměstnance, externí partnery a poskytovatele služeb společnosti, kteří mají přístup k informacím a systémům společnosti. Zahrnuje všechny fyzické a digitální informace, jakož i odpovídající technická a organizační opatření k ochraně těchto informací.

Bamberg, 31.10.2024

- Vedení společnosti -

Stefan Frey

s.frey@ideal-automotive.com, Nov 11,2024 08:11:01 AM UTC

- Pověřenec pro bezpečnost informací -

Martin Schnapp

m.schnapp@ideal-automotive.com, Oct 31,2024 09:14:43 AM UTC