Smernica

o informačnej bezpečnosti

Informácie o dokumente	
Názov	IS1-4 IA Smernica o informačnej bezpečnosti
Skratka dokumentu / odkaz:	IS1-4
Vypracované dňa:	27.09.2024
Posledná zmena dňa:	14.08.2024
Počet strán:	7
Stupeň dôvernosti:	Verejné
Číslo verzie:	2
Stav spracovania:	Freigegeben
Podlieha schváleniu:	Áno
Schválené dňa:	14.08.2024
Schválil: Vedenie podniku (konateľ) / ISB	Schválenie prostredníctvom zdokumentovaného schválenia platnej hlavnej verzie na intranetovej stránke strediska IS od ISB a GF
Predpis vstúpi do platnosti dňa:	01.09.2024
Vlastník dokumentu:	Pracovník poverený informačnou bezpečnosťou (ISB)
Rozsah platnosti:	Celá skupina IDEAL Automotive Gruppe po celom svete (IA)

Obsah

Vedenie podniku týmto schvaľuje nasledujúcu smernicu o informačnej bezpečnosti ako súčasť svojej stratégie:

1. Význam spracúvania informácií

Spracúvanie informácií zohráva kľúčovú rolu pre našu bežnú prevádzku. Všetky podstatné strategické a operatívne funkcie a úlohy zásadne podporuje oddelenie ICT. Výpadok ICT systémov sa musí dať v krátkom čase úplne kompenzovať. Ani v čiastkových oblastiach sa nesmie naša činnosť prerušiť. Keďže naša hlavná kompetencia tkvie v partnerskom vývoji inovatívnych produktov v spolupráci so zákazníkmi a dodávateľmi, má ochrana týchto informácií pred neoprávneným prístupom a pred nepovolenými zmenami existenčný význam.

2. Medziodborové ciele

Dostupnosť našich dát a našich ICT systémov sa zabezpečuje vo všetkých technických a obchodných oblastiach, aby mohli byť tolerované očakávané prestoje. Nesprávna funkcia a nezrovnalosti v dátach a ICT systémoch sú prijateľné iba v malom rozsahu a iba vo výnimočných prípadoch (integrita). Požiadavky na utajovanie sú na bežnej úrovni v súlade s príslušnými zákonnými predpismi. Informácie, ktoré sú na základe internej klasifikácie alebo zmluvných podmienok našich zákazníkov vyhodnotené ako dôverné alebo tajné, sa musia osobitne chrániť.

Štandardné bezpečnostné opatrenia musia byť vo vzťahu k hodnote informácií vhodných na ochranu a ICT systémov ekonomicky opodstatnené. Škodovým udalostiam s vysokými finančnými dôsledkami sa musí predchádzať.

Všetci zamestnanci podniku dodržujú príslušné zákony (napr. zákony a nariadenia o ochrane údajov), interné pracovné postupy a návody a uzavreté zmluvné ustanovenia. Musí sa zabrániť negatívnym finančným a nehmotným následkom pre podnik aj zamestnancov, ktorých príčinou je porušenie zákonov a zmlúv.

Všetci zamestnanci a vedenie podniku sú si vedomí svojej zodpovednosti pri manipulácii s ICT systémami a podporujú bezpečnostnú stratégiu podľa svojich najlepších možností.

2.1 Podrobné ciele

Oneskorené alebo chybné rozhodnutia manažmentu môžu mať ďalekosiahle následky. Preto je pre manažment pri významných rozhodnutiach dôležitý prístup k aktuálnym riadiacim dátam. Pre tieto informácie sa musí zabezpečiť vysoká úroveň bezpečnosti z hľadiska ich dostupnosti a integrity.

Zákony na ochranu údajov a záujmy našich zamestnancov vyžadujú zabezpečenie utajenia údajov zamestnancov. Osobné údaje našich zamestnancov preto podliehajú vysokej ochrane ich dôvernosti. To isté platí pre osobné údaje našich obchodných partnerov.

Údaje o dopytoch a ponukách od a pre našich zákazníkov, ako aj konštrukčné dáta našich zákazníkov a nášho vývojového oddelenia vyžadujú veľmi vysoký stupeň utajenia. Ich stratou alebo krádežou môžu vzniknúť konkurenčné nevýhody alebo nároky na náhradu škody namierené proti nám. Vďaka technickým a organizačným opatreniam a veľkej pozornosti zamestnancov sa chráni dôvernosť informácií a zabraňuje sa manipulácii s nimi.

Pre oblasť logistiky a pre výrobné závody sa zabezpečuje dostupnosť a bezchybnosť systémov. Prestoje sú akceptovateľné len vo veľmi nízkej miere, nakoľko môžu priamo aj nepriamo viesť k znižovaniu výnosov a negatívne vplývať na spokojnosť zákazníkov.

Využívanie internetu a portálových aplikácií na obstarávanie informácií a komunikáciu je pre nás samozrejmosťou. E-mail slúži ako náhrada alebo doplnenie iných spôsobov komunikácie. Príslušnými opatreniami sa zabezpečuje, že riziká využívania sú podľa možnosti čo najnižšie.

3. Manažment informačnej bezpečnosti

Na dosiahnutie cieľov informačnej bezpečnosti bola zriadená organizácia bezpečnosti. Bol vymenovaný pracovník zodpovedný za informačnú bezpečnosť (ISB/CISO). Pracovník zodpovedný za informačnú bezpečnosť je vo svojej funkcii priamo podriadený vedeniu podniku.

Pracovníkovi zodpovednému za informačnú bezpečnosť poskytuje vedenie dostatočné finančné a časové zdroje, aby sa mohol pravidelne ďalej vzdelávať a informovať dosahovať ciele informačnej bezpečnosti stanovené manažmentom.

Bezpečnostných administrátorov ICT a pracovníka zodpovedného za informačnú bezpečnosť musia podporovať používatelia ICT pri výkone svojej práce.

Pracovník zodpovedný za informačnú bezpečnosť musí byť včas zainteresovaný do všetkých projektov, aby sa už vo fáze plánovania zohľadnili príslušné aspekty týkajúce sa bezpečnosti. Ak sa to týka osobných údajov, platí to isté pre pracovníka zodpovedného za ochranu osobných údajov.

Používatelia ICT sa pri nastoľovaní otázok týkajúcich sa bezpečnosti musia pridŕžať pokynov pracovníka zodpovedného za informačnú bezpečnosť.

4. Bezpečnostné opatrenia

Pre všetky postupy, informácie, ICT aplikácie a ICT systémy sa vymenuje zodpovedná osoba, ktorá zisťuje príslušnú potrebu ochrany v spolupráci s pracovníkom zodpovedným za informačnú bezpečnosť.

Pre všetky zodpovedné funkcie sa musia určiť zástupcovia. Inštruktážou a dostatočnou dokumentáciou sa musí zabezpečiť, aby mohli zástupcovia plniť svoje úlohy.

Budovy a priestory sú chránené dostatočnou kontrolou vstupu. Prístup do ICT systémov sa chráni primeranou kontrolou vstupu a prístup k údajom reštriktívnou koncepciou oprávnení.

Ochranné programy proti počítačovým vírusom sa použijú na všetky ICT systémy. Všetky prístupy na internet sa zabezpečia vhodnými firewall systémami. Všetky ochranné programy sa konfigurujú a spravujú tak, aby predstavovali efektívnu ochranu a zabránilo sa prípadnej manipulácii. Okrem toho používatelia ICT podporujú tieto bezpečnostné opatrenia svojím uvedomelým spôsobom práce z hľadiska bezpečnosti a v prípade problémov informujú príslušné určené pracoviská.

So všetkými ICT systémami, aplikáciami a všetkými informáciami sa musí prostredníctvom vhodných technických a organizačných opatrení manipulovať tak, aby sa dali kedykoľvek dosahovať ciele týkajúce sa ochrany. Technické a organizačné opatrenia sa musia pravidelne kontrolovať a v prípade potreby upravovať.

Straty údajov sa nedajú nikdy úplne vylúčiť. Rozsiahlym zabezpečením dát sa preto zabezpečí, že prevádzku ICT možno za krátky čas obnoviť, keď sa stratia časti operatívneho súboru dát alebo sú zjavne chybné. Informácie sa označujú jednotne a ukladajú sa tak, aby sa dali rýchlo nájsť.

Na obmedzenie väčších škôd v dôsledku stavov núdze resp. na ich predchádzanie sa musí na bezpečnostné incidenty reagovať promptne a dôsledne. Opatrenia pre prípad núdze sú pripravené v samostatnej koncepcii prevencie núdzových prípadov. Naším cieľom je aj v prípade výpadku systému zachovať kritické obchodné procesy a obnoviť dostupnosť vypadnutých systémov v tolerovateľnej lehote.

Ak sú ICT služby premiestnené na externé miesta, zadajú sa od nás konkrétne bezpečnostné požiadavky v zmluvách Service Level Agreements. Ak sa na účely plnenia zmlúv musia dodávateľom sprístupniť údaje s vysokou potrebou ochrany, musíme ich osobitne a výslovne zaviazať k ich utajovaniu. Stanovuje sa právo na kontrolu.

Používatelia ICT sa zúčastňujú školení o využití ICT služieb a o súvisiacich bezpečnostných opatreniach. Vedenie podniku pritom podporuje ďalšie vzdelávanie a doškoľovanie.

5. Zlepšenie bezpečnosti

Aktuálnosť a účinnosť systému manažmentu informačnej bezpečnosti sa pravidelne kontroluje. Okrem toho sa pravidelne overuje, či dotknutí zamestnanci poznajú príslušné opatrenia, či sa dajú realizovať a integrovať do prevádzkových procesov.

Vedenie podniku podporuje stále zlepšovanie úrovne bezpečnosti. Zamestnanci sú podnecovaní, aby možné zlepšenia alebo slabé stránky komunikovali na príslušné miesta.

Neustálou revíziou nariadení a ich dodržiavania sa zabezpečí dosiahnutie vytýčenej úrovne bezpečnosti a ochrany údajov. Odchýlky sa analyzujú s cieľom zlepšiť bezpečnostnú situáciu a neustále udržiavať aktuálny stav ICT bezpečnostnej techniky.

6. Dôsledky pri nedodržiavaní

Nedodržiavanie ustanovení tejto smernice môže znamenať závažné následky pre firmu. Porušenia smernice môžu mať – podľa závažnosti a situácie – za následok disciplinárne alebo právne konzekvencie.

7. Odkaz na Vyhlásenie IA o zásadách

Tejto smernici je nadriadené Vyhlásenie IDEAL Automotive o zásadách, ktoré sa pravidelne kontroluje a v prípade potreby upravuje. Všetci zamestnanci sú povinní informovať sa o aktuálnom obsahu vyhlásenia o zásadách a zabezpečiť, aby ich konanie bolo neustále v súlade s princípmi, ktoré sú stanovené v tomto vyhlásení.

8. Postup v prípade zmien

Zmeny smernice o informačnej bezpečnosti sa vykonávajú systematicky a transparentne. Každú plánovanú zmenu najprv overí a schváli manažment informačnej bezpečnosti. Nový alebo zmenený obsah sa integruje do nášho programu školení, aby sa zabezpečilo, že príslušné predpisy budú pochopené a aplikované.

9. Rozsah platnosti

Táto smernica platí pre všetkých zamestnancov, externých partnerov a poskytovateľov služieb našej spoločnosti, ktorí majú prístup k jej informáciám a systémom. Zahŕňa všetky fyzické a digitálne informácie a príslušné technické a organizačné opatrenia na ochranu týchto informácií.

Bamberg, 31.10.2024

- Vedenie (konateľ) -

Stefan Frey

s.frey@ideal-automotive.com, Nov 11,2024 08:09:59 AM UTC

- Pracovník zodpovedný za informačnú bezpečnosť -

Martin Schnapp

m.schnapp@ideal-automotive.com, Oct 31,2024 09:15:01 AM UTC