Constellium

POLITIKA BEZPEČNOSTI INFORMACÍ

Organizace Constellium Extrusions Děčín s.r.o. zahrnující i odloučená pracoviště si je vědoma své odpovědnosti vůči všem zainteresovaným stranám, a proto vyhlašuje svoji Politiku bezpečnosti informací.

Závazek vedení

Vedení Constellium Extrusions Děčín s.r.o. (dále jen „DEC“) se zavazuje podporovat zavedení a provoz systému řízení bezpečnosti informací (dále jen „ISMS“), a to stanovením Politiky bezpečnosti informací organizace, stanovením cílů ISMS a plánu na jejich dosažení, stanovením rolí, povinností a odpovědností v oblasti bezpečnosti informací, propagací významu plnění cílů bezpečnosti v rámci organizace, zajištěním potřebných zdrojů, stanovením kritérií pro akceptaci rizik a akceptovanou úroveň rizika, zajištěním provádění interních auditů ISMS a prováděním přezkoumání ISMS vedením organizace.

Základní charakteristika bezpečnosti informací

Bezpečnost informací je charakterizována jako zachování důvěrnosti, integrity a dostupnosti informací, přičemž:

a. důvěrnost je zajištění toho, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům,
b. integrita je zabezpečení přesnosti a úplnosti informace a metod jejího zpracování,
c. dostupnost je zajištění toho, že informace je přístupná a použitelná na žádost oprávněného jednotlivce, entity nebo procesu.

Cíle a význam bezpečnosti informací v organizaci

Cílem ISMS v DEC je zajištění dostupnosti informačních aktiv jen oprávněným osobám, správnosti a kompletnosti informací, důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, proti neoprávněnému přístupu, změnám nebo šíření, a to v souladu se zákony a jinými právními předpisy ČR.

Bezpečnostní strategie organizace

Systém řízení bezpečnosti informací je zaveden v souladu s normou ČSN ISO/IEC 27001:2014 a v rozsahu implementace opatření dle přílohy A této normy v závislosti na výsledcích hodnocení rizik.

Základní definice odpovědností

Vedení organizace definuje funkce, kterým jsou přiděleny příslušné role, odpovědnosti a pravomoci pro řízení bezpečnosti informací.

Výbor pro řízení bezpečnosti informací (dále jen „Výbor") - je tvořen osobami s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení a rozvoj ISMS a osobami významně se podílejícími na řízení a koordinaci činností spojených s bezpečností informací. Členem Výboru musí být vždy alespoň jeden zástupce vrcholového vedení organizace nebo jím pověřená osoba a Manažer bezpečnosti informací. Pravomoci výboru zastává v případě společnosti Constellium porada vedení této společnosti.

Manažer bezpečnosti informací – odpovídá vedení organizace. Realizuje bezpečnostní zásady Politiky bezpečnosti informací organizace a navrhuje její změny, sleduje dodržování bezpečnostních opatření a realizaci jejich změn, zabezpečuje hodnocení rizik, řešení bezpečnostních incidentů a zvyšování bezpečnostního povědomí zaměstnanců organizace.

Garant aktiva – je bezpečnostní role odpovědná za definici požadavků na rozvoj, použití a bezpečnost primárního nebo podpůrného aktiva

Auditor bezpečnosti informací – zaměstnanec, který je určen jako interní auditor ISMS organizace.

Posouzení rizik a požadavky na bezpečnost informací

Hodnocení aktiv se provádí z hlediska požadavků na jejich důvěrnost, dostupnost a integritu. Posouzení rizik je prováděno na základě identifikace, analýzy a hodnocení rizik a má za cíl určit možné hrozby, zranitelnosti a rizika hodnoceného systému, odhadnout ztráty, které mohou vzniknout působením hrozeb na informační aktiva zařazená do ISMS organizace. K pokrytí zjištěných rizik, předcházení nebo snížení nežádoucích následků a k dosažení neustálého zlepšování se přijímají bezpečnostní opatření (Prohlášení o aplikovatelnosti, Plán zvládání rizik). Posuzování rizik a hodnocení aktiv se provádí pravidelně jednou za tři roky nebo v případě větších změn v posuzované oblasti.

Požadavek na školení a vzdělávání

Organizace dohlíží na to, aby zaměstnanci, kterých se týkají povinnosti definované v ISMS, byly odborně způsobilí k výkonu požadovaných úkolů. Způsobilost je udržována školením či vzděláváním dle profesí, v intervalech stanovených v platných předpisech.

Interní audit

K zajištění ochrany provozovaných informačních systémů a systému ISMS je prováděn pravidelný audit bezpečnosti informací. Auditní požadavky a činnosti zahrnující kontrolu ISMS organizace jsou plánovány Auditorem bezpečnosti informací a schváleny vedením společnosti v periodě minimálně 1 x ročně.

Pravidelné přezkoumání

Přezkoumání systému managementu bezpečnosti informací se provádí s cílem zajistit účelnost, adekvátnost a efektivnost provozovaného ISMS v organizaci. Přezkoumání ISMS zároveň uvádí možnosti zlepšení a návrh změn v provozovaném ISMS. Interval přezkoumání ISMS je v DEC stanoven na 1x ročně.

Uvedení důsledků v případě nedodržení politiky

Všichni zaměstnanci jsou seznámeni se skutečností, že nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance a v některých případech i jako přestupek nebo trestný čin.

Způsob revize

Politika bezpečnosti informací je pro všechny pracovníky k dispozici na podnikovém intranetu a pro externí partnery na internetových stránkách společnosti. Revize bezpečnostní politiky je prováděna jejím vlastníkem minimálně 1x ročně nebo při významné změně ovlivňující její aktuálnost a platnost. Datum vydání platné revize je vyjádřeno datem vydání bezpečnostní politiky.

Navazující dokumentace

Na Politiku bezpečnosti informací, navazuje dokumentace ISMS rozpracovávající opatření pro oblasti bezpečnosti informací. Tyto dokumenty obsahují konkrétní odpovědnosti za realizaci procesů a činností bezpečnosti informací.

Hierarchie dokumentace ISMS v DEC je následující:

1. Politika bezpečnosti informací (tato politika),
2. Směrnice bezpečnosti informací a Uživatelská bezpečnostní směrnice
3. Záznamy pro podporu ISMS (zejména dokumentace hodnocení rizik, dokumentace bezpečnostních zón, dokumentace spojená s dodavateli, evidence bezpečnostních incidentů, plán kontinuity činností, dokumentace interních auditů ISMS, evidence neshod a pravidelné přezkoumání stavu bezpečnosti informací).

Řízení dokumentace ISMS je popsáno v organizačních směrnicích ISŘ-22 a VS-09.

Jiří Palma	Miloslav Šoltys	Jan Bibík	Libor Voborský	Jan Šipal
jednatel společnosti	technický ředitel	výrobní ředitel	obchodní ředitel	finanční ředitel

Dne 1.2.2024