ALVA Strakonice

Úvod

Politika bezpečnosti informací deklaruje základní cíle a principy řízení bezpečnosti informací ve společnosti ALVA Strakonice s.r.o.

Cíle, předmět a principy

Hlavním cílem řízení bezpečnosti informací je zajištění ochrany klíčových informačních aktiv společnosti ALVA Strakonice s.r.o., které jsou nezbytným nástrojem pro plnění strategie společnosti.

Informačními aktivy rozumíme informace potřebné k zajištění činnosti společnosti a všechny zdroje, které jsou nezbytné pro pořizování, zpracování, ukládání a k využívání informací i k jejich vlastní ochraně. Jedná se zejména o data, informace, software, hardware, koncová zařízení (počítače, notebooky, tiskárny, čtečky čárového kódu apod.), infrastrukturu (sítě, síťová zařízení apod.), osoby (interní i externí pracovníci pracující s informačními aktivy), dodavatele (správci HW, SW apod.). Informační aktiva zahrnují i informace zpracovávané jinak než v elektronické podobě (tištěné dokumenty a záznamy, záznamové knihy, video-záznamy z bezpečnostních kamer apod.).

Princip zajištění bezpečnosti informací tkví v identifikaci podstatných informačních aktiv, zjištění všech aspektů, které mohou tato aktiva ohrozit, a v přijetí dostatečných opatření pro zajištění požadované dostupnosti, důvěrnosti, integrity a autenticity těchto aktiv.

Cílové skupiny

Řízení bezpečnosti informací společnosti se dotýká všech zainteresovaných stran, zejména všech interních a externích pracovníků, dodavatelů a zákazníků. Každý, kdo přichází do styku s informačními aktivy společnosti, musí být s touto politikou seznámen a musí být v potřebném rozsahu seznámen s konkrétními požadavky, pravidly a postupy pro zacházení s informačními aktivy obsaženými v řídící dokumentaci společnosti.

Zásady řízení bezpečnosti informací

Veškeré podstatné aspekty bezpečnosti informací jsou dokumentovány v interní řídící dokumentaci společnosti. Jsou pravidelně přehodnocovány, aktualizovány a schvalovány vedením společnosti a tvoří jednotný systém řízení bezpečnosti informací.

Za řízení bezpečnosti informací na nejvyšší úrovni zodpovídá určený jednatel společnosti, který zároveň vykonává roli Bezpečnostního manažera.

Základní zásady upravené v systému řízení bezpečnosti informací jsou:

1. Společnost přijímá a prosazuje opatření potřebná pro zajištění bezpečnosti informací na základě příkladů nejlepší praxe, zejména v souladu s požadavky standardu na systém řízení bezpečnosti informací dle ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací a ČSN ISO/IEC 27002:2013 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací.

2. Informační aktiva společnosti jsou identifikována a přezkoumána v rámci analýzy rizik z hlediska případných dopadů na společnost při porušení jejich dostupnosti, důvěryhodnosti a důvěrnosti.
3. Veškeré informace jsou vždy klasifikovány a označovány stupněm jejich důvěrnosti.
4. Použití informačních aktiv je vždy řízeno v souladu s jejich klasifikací a to včetně řízení přístupu k nim. Přístup k informačním aktivům je vždy udělován výhradně na základě účelu, ke kterému je aktivum využíváno. Pokud účel použití informačního aktiva pomine, musí být přístup zrušen.
5. Ochrana fyzického prostředí zajišťuje dostatečný základ pro zajištění ochrany informačních aktiv.
6. Koncoví uživatelé informačních aktiv jsou poučeni o předepsaných postupech a pravidlech v souvislosti s používáním informačních aktiv.
7. Dodavatelé a zákazníci jsou seznámeni se systémem řízení bezpečnosti informací v rozsahu potřebném pro zajištění bezpečnosti informačních aktiv používaných v dodavatelsko-odběratelských vztazích se společností ALVA Strakonice s.r.o., včetně zajištění bezpečnosti informací zákazníků společnosti využívaných ALVA Strakonice s.r.o. pro plnění dodávek. Podstatné aspekty bezpečnosti informací v rámci dodavatelsko-odběratelských vztahů jsou smluvně upraveny.
8. Jakékoliv porušení bezpečnosti informací či jen podezření na takové porušení musí všechny zainteresované strany neprodleně ohlásit Bezpečnostnímu manažerovi, který zajistí jeho přezkoumání a záznam.