BEZPEČNOSTNÍ POLITIKA ISMS

Společnost KARSIT HOLDING, s.r.o. působí v oblasti vývoje a výroby lisovaných, svařovaných a lakovaných dílů pro automobilový průmysl se zaměřením na výrobu panelových dílů a kovových konstrukcí karoserií a autosedadel.

Společnost KARSIT, s.r.o. se zavazuje, že:

1) Hlavním cílem organizace KARSIT, s.r.o. je zajištění bezpečnosti informací pomocí přiměřených a odpovídajících opatření, která budou chránit informační aktiva tak, aby poskytly odpovídající míru jistoty.
2) Tímto dokumentem se vedení těchto organizací přihlašuje k implementaci procesů informační bezpečnosti (ISMS), včetně nezbytné podpory finanční, materiální a personální.
3) Tento cíl je naplňován vybudováním, zavedením, provozováním, kontrolováním, údržbou a neustálým zlepšováním dokumentovaného systému řízení bezpečnosti informací v kontextu aktivit a rizik výše uvedených společností.
4) Základními zdroji pro řízení bezpečnosti informací v rámci organizací jsou právní předpisy, standardy, normy a doporučení, které musí být v procesu řízení bezpečnosti informací respektovány.
5) ´Pojmem bezpečnost informací rozumíme proces zajišťování ochrany informací na potřebné úrovni z hlediska jejich důvěrnosti, integrity a dostupnosti.
6) Pro zajištění všech požadovaných úkolů, případně plnění legislativních požadavků, vytváříme, zpracováváme a udržujeme informace různého charakteru, které vyžadují adekvátní úroveň ochrany.
7) Organizace naplňují jednotlivé bezpečnostní cíle pomocí adekvátních opatření, určených v rámci procesu řízením rizik bezpečnosti informací v oblastech organizace bezpečnosti, klasifikace informací, personální a fyzické bezpečnosti, bezpečnosti prostředí, bezpečnosti řízení komunikací a provozu, řízení bezpečnosti přístupu, bezpečnosti vývoje a údržby systémů, řízení kontinuity provozu a souladu s legislativními požadavky, tak, jak je vymezeno v Bezpečnostní politice organizace.

Úvodní ustanovení

1. Tato Bezpečnostní politika organizací KARSIT, s.r.o., (dále jen organizace) zavádí pravidla v oblasti systému řízení bezpečnosti informací (dále jen „Pravidla“), která jsou základním strategickým dokumentem zajišťujícím rámec informační bezpečnosti organizace.
2. Pravidla se vztahují na veškeré informační systémy a veškeré informace, které jsou v rámci organizace zpracovávány (dále jen „informační aktiva“). Cílem těchto Pravidel je zejména:
    a) určit cíle informační bezpečnosti,
    b) určit hlavní zásady informační bezpečnosti,
    c) určit bezpečnostní potřeby organizace,
    d) určit dokumentaci informační bezpečnosti,
    e) určit systém řízení bezpečnosti informací, tj. práva a povinnosti ve vztahu k řízení bezpečnosti informací,
    f) zavádění bezpečnostních opatření na základě bezpečnostních potřeb a výsledků hodnocení rizik.

3. Vedení organizace se tímto dokumentem hlásí k naplňování a dodržování všech zásad informační bezpečnosti, které jsou definovány v tomto a ostatních dokumentech bezpečnostní politiky.

Cíle Bezpečnostní politiky organizace

1. Zajištění požadované úrovně ochrany dostupnosti, důvěrnosti a integrity informačních aktiv organizace. Veškeré významné uživatelské operace nad aktivy jsou jednoznačně identifikovány, bezpečně zaznamenávány a následně vyhodnocovány.
2. Schopnost detekovat kybernetické bezpečnostní incidenty, a to včetně identifikace původce bezpečnostního incidentu, způsobu narušení bezpečnosti, dopadů a přijmutí příslušných reaktivních bezpečnostních opatření.
3. Zavedení a řízení bezpečnostních opatření a udržování aktualizované bezpečnostní dokumentace.
4. Aplikovat procesní rámec řízení informační bezpečnosti v organizaci.

BEZPEČNOSTNÍ POLITIKA ISMS

Hlavní zásady Bezpečnostní politiky

1. Zajištěním bezpečnosti informací se pro účely této politiky rozumí zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojené priority, typicky autentičnost, odpovědnost, nepopiratelnost a spolehlivost.
2. Informační bezpečnost je v organizaci chápána jako komplexní proces ochrany aktiv tvořený opatřeními personální bezpečnosti, fyzické bezpečnosti, bezpečnosti informačních technologií, plánováním kontinuity činností a zajištěním souladu s požadavky legislativy.
3. Jsou jasně stanovena pravidla, kompetence a odpovědnosti v oblasti informační bezpečnosti a každý zaměstnanec je s nimi seznámen.

Bezpečnostní potřeby

1. Bezpečnostní potřeby pro jednotlivá informační aktiva vychází z jejich kategorizace na základě předchozího ohodnocení a dále z klasifikace zpracovávaných informací.

Bezpečnostní politika

1. Celkový systém bezpečnostní politiky v organizaci je vypracován v souladu:
    a) s mezinárodní normou ČSN ISO/IEC 27001:2014 – Systém řízení bezpečnosti informací,
    b) se zákonem na ochranu osobních údajů č. 110/2019 Sb.
    c) s Nařízením EP a rady EU 2016/679 - GDPR
    d) ostatními požadavky danými obecně závaznými právními předpisy,
    e) úrovní rizik, která hrozí prostředkům (informacím) organizace,
    f) potřebami organizace v oblasti zpracování a ochrany informací.

2. Bezpečnostní politiku tvoří dokumenty tří úrovní:
    a) Politiky – začleňují bezpečnost informací do kontextu celkové bezpečnosti organizace a definují základní bezpečnostní principy,
    b) Směrnice – obsahují zpravidla popis realizace vybraných bezpečnostních prvků a bezpečnostních opatření pro konkrétní principy politiky a konkrétní standardy. Obsahují technické údaje popisující použitý software, hardware, použitá procedurální či organizační opatření a způsob jejich implementace.
    c) Pracovní a procesní postupy – Definují pracovní postupy nezbytné pro dodržení bezpečnostních standardů.

Systém řízení bezpečnosti informací

1. Systém řízení bezpečnosti informací je založen na mezinárodní normě ČSN ISO/IEC 27001:2014 – ISMS.
2. K zajištění informační bezpečnosti v organizaci jsou definovány následující role:
    a) manažer kybernetické bezpečnosti,
    b) auditor kybernetické bezpečnosti,
    c) garant aktiva,
    d) výbor pro řízení informační bezpečnosti.
3. V organizaci jsou prováděna nezávislá přezkoumání formou auditu:
    a) celkového systému řízení informační bezpečnosti (ISMS)
    b) aktuálnosti a správnosti bezpečnostní dokumentace
    c) aktuálního stavu bezpečnostních opatření
    d) dle aktuální potřeby
4. V organizaci jsou řízena aktuální rizika informačních aktiv a k nim stanoveny relevantní hrozby, zranitelnosti a možné dopady.

BEZPEČNOSTNÍ POLITIKA ISMS

Oblasti relevantní pro implementaci ISMS – hranice

1. Pro organizaci jsou definované hranice ISMS v areálu sídla společnosti a to Jaromírova č.p.91, 551 01 Jaroměř - Jakubské Předměstí
2. Implementace je aplikována na celou organizační strukturu.
3. Pro organizaci je definovaný rozsah ISMS níže uvedeným výčtem:
    1. politiky bezpečnosti informací,
    2. organizace bezpečnosti informací,
    3. bezpečnost lidských zdrojů,
    4. řízení aktiv,
    5. řízení přístupu,
    6. kryptografie,
    7. fyzická bezpečnost a bezpečnost prostředí,
    8. bezpečnost provozu,
    9. bezpečnost komunikací,
    10. akvizice, vývoj a údržba systémů,
    11. vztahy s dodavateli,
    12. řízení incidentů bezpečnosti informací,
    13. aspekty řízení kontinuity,
    14. soulad s požadavky.

V Jaroměři 01.03.2022

.....	.....
Martin Horký	**Vit Kaiser**