

POLITIKA INTEGROVANÉHO SYSTÉMU ŘÍZENÍ

Rodinný podnik IMS-Drašnar s.r.o., nástrojárna a lisovna plastů, je spolehlivým dodavatelem kvalitních výrobků a služeb na tuzemském i zahraničním trhu.

Integrovaný systém řízení zahrnuje všechny systémy řízení dle norem ISO 9001, IATF 16949, ISO 14001, zohledňuje požadavky na BOZP a PO, bezpečnost informací (TISAX), GDPR, Ochranu oznamovatelů (Whistleblowing), ESG a společenskou odpovědnost.

SYSTÉM MANAGEMENTU KVALITY

- Orientace na zákazníka
 - plnění požadavků v požadované kvalitě a termínu
 - přezkoumávání požadavků
 - proaktivní přístup
- Neustálé zlepšování a inovace
 - zlepšování systému řízení
 - modernizace strojů a technologií
 - vzdělávání zaměstnanců
- Dodržování požadavků norem a platné legislativy
 - certifikace dle ISO 9001, IATF 16949, ISO 14001, TISAX
 - spolupráce s externími konzultanty
- Hodnocení dodavatelů
 - zvyšování náročnosti vůči dodavatelům
- Rozvoj zaměstnanců
 - zvyšování povědomí o ISŘ
 - vzdělávání a možnost kariérního růstu
- zdůrazňování osobní odpovědnosti za kvalitu

SYSTÉM ENVIRONMENTÁLNÍHO MANAGEMENTU (EMS)

- Plnění zákonných požadavků
- Zohlednění požadavků na ochranu životního prostředí ve všech procesech
- Minimalizace dopadů na životní prostředí
 - analýza vyrobitelnosti (materiály, technologie, množství odpadu)
 - snižování množství nerecyklovatelného odpadu, pečlivé třídění a odprodej k recyklaci
 - snižování spotřeby elektrické energie a plynu – využívání odpadního tepla z výroby
 - množstvím zeleně a vodními plochami snižovat teplotu okolí
- Prohlubování znalostí zaměstnanců a jejich zapojování do ochrany životního prostředí

BEZPEČNOST A OCHRANA ZDRAVÍ PŘI PRÁCI A POŽÁRNÍ OCHRANA (BOZP a PO)

- Dodržování legislativy v oblasti BOZP a PO
- Analýza rizik a přijímání opatření vedoucí k eliminaci nebo minimalizaci těchto rizik
- Modernizace zařízení, strojů a používaných technologií
- Zavádění nových pracovních postupů a technologií z hlediska vyšší bezpečnosti a požární ochrany

OCHRANA OSOBNÍCH ÚDAJŮ (GDPR)

- Dodržování právních požadavků na ochranu osobních údajů
- Spolupráce s odborným garantem a konzultantem v oblasti GDPR

ESG (Environmental, Social & Governance) a společenská odpovědnost

- Dodržování legislativy a požadavků zákazníků
- Integrace principů ESG do všech oblastí podnikání
- Naplňování vybraných Cílů udržitelného rozvoje OSN
- Dodržování Etického kodexu i Etického kodexu rodinného podniku
 - dodržování lidských práv
 - zákaz korupce a neetického jednání se zainteresovanými stranami
 - zákaz nelegálního zaměstnávání, dětské práce, diskriminace a šikany
 - zapojení do veřejného života, spolupráce s obcí, školami a spolky

WHISTLEBLOWING (OCHRANA OZNAMOVATELŮ)

- Interní oznamovací systém protiprávního jednání a ochrana oznamovatelů jsou zavedeny v souladu s právními požadavky
- Nad rámec zákona je okruh možných oznamovatelů je rozšířen i o obchodní partnery

POLITIKA BEZPEČNOSTI INFORMACÍ (ISMS)

(ISMS information security management system/ systém řízení bezpečnosti informací)

Cílem politiky ISMS je chránit informační aktiva společnosti proti všem vnitřním, vnějším, úmyslným nebo náhodným hrozbám.

Závazek vedení organizace

Organizace se zavazuje, že bude prosazovat tuto politiku a v souladu s ní

- Pravidelně monitorovat a vyhodnocovat bezpečnostní rizika a přijímat odpovídající opatření vedoucí k omezení jejich vlivu
- Neustále zlepšovat systém bezpečnosti informací, zabezpečovat včasnou dostupnost informací a zamezit nežádoucí modifikaci, zneužití nebo ztrátě informací,
- Definovat způsob zpracování informací vnitřními předpisy a dokumentovanými postupy, které jsou součástí řízené dokumentace

Odpovědnost zaměstnanců

- Každý zaměstnanec, kterému byl umožněn přístup k informačním prostředkům pro potřeby výkonu pracovní činnosti, přebírá odpovědnost za bezpečné nakládání s těmito prostředky a za ochranu informací ve své působnosti.
- Stanovená, přijatá a schválená politika a související bezpečnostní dokumentace je závazná pro všechny uživatele s přístupem k informacím, a to bez ohledu na zastávanou funkci, pozici či roli v Organizaci.
- Všichni uživatelé nesou v souladu s platnou legislativou a předpisy svůj díl zodpovědnosti za dodržení, resp. porušení pravidel, s nimiž byli seznámeni.
- Všichni zaměstnanci jsou povinni předepsaným způsobem reagovat na závady, poruchy a bezpečnostní incidenty, které se vyskytnou a upozornit na ně v souladu s příslušnými vnitřními předpisy.

Hlavní zásady systému bezpečnosti informací a způsob jejich zabezpečení

- Zajistit ochranu osobních dat v souladu s platnou legislativou
- Vytvářet a prosazovat systém řízeného přístupu k informacím
- Začleňovat zabezpečení informací do odpovědnosti za práci
- Zajišťovat vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací
- Provádět stálou identifikaci bezpečnostních incidentů a přijímat účinná opatření pro zlepšování bezpečnosti informací
- Prosazovat bezpečnostní pravidla pro přenosná počítačová zařízení a jiné nosiče informací
- Zajišťovat pravidelné zálohování dat a ty ukládat na bezpečném místě
- Zajišťovat politiku bezpečného pracoviště, zajišťovat spolehlivou kontrolu celé integrity počítačové sítě

V České Třebové 06.09.2024



Lucie Vejdová, jednatel firmy