Politika Bezpečnosti Informací

Účel

Tato Politika bezpečnosti informací stanovuje závazný rámec pro řízení kybernetické a informační bezpečnosti ve společnosti. Je vydána v souladu s legislativou (ZOKB a související předpisy, zákon č. 224/2015 Sb., o prevenci závažných havárií), s požadavky na regulované služby a s normativními požadavky TISAX pro úroveň 2.

Závazek společnosti

Společnost jako velký podnik zajišťuje, že jsou všechna informační aktiva chráněna způsobem odpovídajícím jejich významu. Zajišťujeme bezpečnost informací jak v roli dodavatele, tak v roli poskytovatele služeb v automobilovém průmyslu.

Vedení společnosti se zavazuje poskytovat potřebné zdroje, podporovat efektivní fungování systému řízení bezpečnosti informací (ISMS) a aktivně přispívat k jeho rozvoji.

Hlavní cíle ISMS

Cílem systému řízení bezpečnosti informací je:

- zajistit **dostupnost, integritu a důvěrnost** všech informací v elektronické i listinné podobě,
- zajistit bezpečný a spolehlivý provoz informačních technologií podporujících činnosti společnosti,
- chránit citlivé informace společnosti a jejích zákazníků, partnerů a dodavatelů,
- splnit požadavky legislativy, smluvních závazků a standardů TISAX.

Zásady řízení bezpečnosti informací

Společnost se zavazuje:

1. Řídit rizika – soustavně identifikovat, vyhodnocovat a minimalizovat rizika v oblasti bezpečnosti informací a ochrany dat.
2. Školit zaměstnance – zajistit odbornou způsobilost všech zaměstnanců prostřednictvím pravidelného školení a vzdělávání dle profesí.
3. Provádět audity – jednou ročně provést audit bezpečnosti informací a napravovat zjištěné nedostatky.
4. Zlepšovat ISMS – neustále zvyšovat účinnost a efektivitu bezpečnostních opatření a procesů.
5. Monitorovat a přezkoumávat systém – pravidelně vyhodnocovat účinnost ISMS, zavádět potřebné změny a reagovat na nové hrozby a požadavky.
6. Respektovat právní a smluvní požadavky – dodržovat platnou legislativu, interní předpisy, smluvní povinnosti a požadavky zainteresovaných stran.
7. Zajišťovat bezpečnost informačních systémů – zavádět a dokumentovat bezpečnostní opatření, řídit přístupy, technologie a procesy.

Odpovědnosti

Společnost podporuje fungování ISMS prostřednictvím:

- stanovení této politiky a souvisejících cílů,
- vymezení rolí, povinností a odpovědností v oblasti bezpečnosti informací,
- systematického školení zaměstnanců a podpory bezpečnostního povědomí,
- zajištění potřebných zdrojů (personálních, technických i finančních),
- stanovení kritérií pro akceptaci rizik a jejich tolerovanou úroveň,
- provádění interních auditů a hodnocení bezpečnosti,
- aktivního řízení bezpečnostních událostí a incidentů,
- podpory neustálého zlepšování ISMS.