

## Politika Bezpečnosti Informací

Společnost SBS – NEPRON, s.r.o. je jedním z předních systémových partnerů v oblasti přenosové techniky a mechatroniky.

Hlavním cílem systému řízení bezpečnosti informací je zajistit bezpečnost citlivých informací z pozice dodavatele a poskytovatele služeb v automobilovém průmyslu. Systém řízení bezpečnosti informací je zaveden v souladu s posouzením shody s požadavky TISAX. Obecným cílem je zajistit spolehlivost a bezpečnost informačních technologií provozovaných pro podporu činností organizace a manipulaci informací v elektronické a listinné formě.

Společnost dbá na to, aby zaměstnanci, kterých se týkají povinnosti definované v systému řízení bezpečnosti informací, byli odborně způsobilí k výkonu požadovaných úkolů. Způsobilost je udržována školením či vzděláváním dle profesí, v intervalech stanovených v platných předpisech.

Vedení organizace zajišťuje trvalou podporu a vyčleňuje potřebné zdroje pro provoz systému řízení bezpečnosti informací.

Nepřetržitě posuzujeme a hodnotíme rizika v oblasti bezpečnosti informací a ochrany dat a přijímáme opatření k odstranění nebo minimalizaci těchto rizik.

K zajištění ochrany provozovaných informačních systémů a systému řízení bezpečnosti informací jednou ročně provádíme pravidelný audit bezpečnosti informací.

Usilujeme o neustálé zlepšování řízení bezpečnosti informací, ochrany osobních údajů, trvalou ochranu svých aktiv a zvládnutí bezpečnostních událostí a incidentů.

Pravidelně provádíme přezkoumání systému řízení bezpečnosti informací s cílem zajistit vhodnost, přiměřenost a efektivitu tohoto systému v naší společnosti. Přezkoumání systému řízení bezpečnosti informací zároveň uvádí možnosti zlepšení a návrh změn v tomto systému.

V rámci naší činnosti respektujeme a dodržujeme relevantní právní požadavky, smluvní bezpečnostní závazky, požadavky zainteresovaných stran pro oblast bezpečnosti informací a ochranu osobních údajů.

Společnost se zavazuje podporovat zavedení a provoz systému řízení bezpečnosti informací a to:

- stanovením Politiky Bezpečnosti informací,
- stanovením cílů systému řízení bezpečnosti informací a plánu na jejich dosažení,
- stanovením rolí, povinností a odpovědností v oblasti bezpečnosti informací,
- propagací významu plnění cílů bezpečnosti v rámci naší společnosti a systematické školení zaměstnanců,
- zavedením a zdokumentováním bezpečnostních opatření,
- zajištěním potřebných zdrojů,
- stanovením kritérií pro akceptaci rizik a tolerovanou úroveň rizika,
- zajištěním provádění interních auditů,
- prováděním hodnocení stavu bezpečnosti prostřednictvím přezkoumání systému řízení bezpečnosti informací vedením organizace,
- neustálým zlepšováním řízení bezpečnosti informací.