



## **POLITIKA ISMS**

Vedení společnosti OSTROJ a.s. vyhláší tuto

### **Politiku managementu bezpečnosti informací**

v souladu s požadavky normy

ČSN EN ISO/IEC 27001 a požadavky TISAX

Vedení společnosti OSTROJ a.s. (dále jen Společnost) se zavazuje:

- Plánovat a uvolňovat zdroje na rozvoj a trvalé zlepšování účinnosti systému managementu bezpečnosti informací.
- Podporovat všemi vhodnými prostředky managementu neustálé zvyšování efektivity systému managementu bezpečnosti informací.
- Pravidelně a systematicky hodnotit rizika v oblasti bezpečnosti informací a nastavovat účinná opatření k jejich eliminaci.
- Pravidelně plánovat Cíle managementu bezpečnosti informací, sledovat a přezkoumávat jejich plnění a využívat je jako důležitý nástroj zlepšování a prevence vzniku bezpečnostních incidentů.
- Zajistit povědomí všech pracovníků firmy o významu systému managementu bezpečnosti informací pro rozvoj Společnosti a pro získávání důvěry zákazníků.
- Zajistit povědomí všech pracovníků firmy o významu všech realizovaných činností vedoucích k zajištění trvalé, stabilní a trvale se zlepšující bezpečnosti informací poskytované firmou zákazníkům.
- Pravidelně přezkoumávat účinnost systému managementu bezpečnosti informací a akceptovat příležitosti pro zlepšování systému managementu bezpečnosti informací.
- Spolupracovat úzce s partnery a dodavateli s cílem integrovat snažení vedoucí k zajištění plánovaných kritérií bezpečnosti informací.
- Využívat požadavků a doporučení zákazníků k rozvoji systému managementu bezpečnosti informací.
- Aplikovat požadavky zákonných norem na ochranu osobních údajů.
- Zřídit důvěrný kanál pro podávání zpráv o porušování politiky informační bezpečnosti, tematicky specifických politik nebo postupů v oblasti informační bezpečnosti (whistleblowing).

V Opavě dne 1.11.2024

Ing. Aleš Martínek  
generální ředitel