POLITIKA SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ
HOLDINGU SPOLEČNOSTÍ ROSTRA

Vrcholové vedení společnosti ROSTRA s.r.o. si uvědomuje důležitost ochrany informací a bezpečnosti dat. Zavazuje se k porozumění rizikům spojeným s informačními aktivy, k dlouhodobému zlepšování bezpečnostních opatření a ke zvyšování efektivity správy informační bezpečnosti.

Politika je závazná pro všechny společnosti holdingu:

- **ROSTRA Stamping s.r.o.**
- **ROSTRA Tools s.r.o.**
- **ROSTRA Group s.r.o.**

Vedení společnosti ROSTRA s.r.o. stanovilo následující zásady:

- Plánovat, zajišťovat a přidělovat odpovídající zdroje pro správu a neustálé zlepšování systému managementu informační bezpečnosti.
- Pravidelně a systematicky identifikovat, hodnotit a řídit rizika, která mohou ohrozit důvěrnost, integritu a dostupnost informací.
- Stanovovat měřitelné **cíle v oblasti bezpečnosti informací**, sledovat jejich naplňování a využívat výsledky jako nástroj prevence bezpečnostních incidentů.
- Zvyšovat **povědomí zaměstnanců** o důležitosti správného zacházení s informacemi prostřednictvím školení, komunikace a podpory odpovědného přístupu.
- Zajistit, aby všichni zaměstnanci i externí subjekty byli seznámeni s příslušnými pravidly, odpovědnostmi a důsledky porušení požadavků informační bezpečnosti.
- Dodržovat právní, smluvní a regulatorní požadavky v oblasti ochrany informací, včetně ochrany osobních údajů dle nařízení **GDPR** a relevantních zákonů ČR/EU.
- Spolupracovat s dodavateli, zákazníky a dalšími partnery s cílem zajistit bezpečnost informací napříč celým dodavatelským řetězcem.
- Provádět pravidelné přezkoumání účinnosti systému ISMS, reagovat na incidenty a identifikované nedostatky a realizovat nápravná a preventivní opatření.
- Integrovat požadavky na bezpečnost informací do všech klíčových procesů v organizaci – od vývoje, nákupu, IT správy, až po logistiku a výrobu.
- Udržovat aktuální řízenou dokumentaci systému bezpečnosti informací a zajistit její dostupnost všem oprávněným osobám.

<u>Od zaměstnanců vedení očekává:</u>

- Chránit přístupová hesla, zařízení, technická data i fyzické záznamy před neoprávněným přístupem.
- Dodržovat stanovená pravidla informační bezpečnosti, interní směrnice a používat firemní systémy výhradně k pracovním účelům.
- Hlásit veškeré bezpečnostní incidenty nebo podezření na porušení bezpečnostních pravidel nadřízenému nebo odpovědné osobě.
- Aktivně přispívat k bezpečnému pracovnímu prostředí a ochraně informací společnosti, zákazníků a partnerů.

NAŠE BUDOUCNOST JE V BEZPEČNOSTI INFORMACÍ PRO UDRŽITELNÝ ROZVOJ A OCHRANU NAŠICH DIGITÁLNÍCH AKTIV.

Vizovice 15.3.2025

Petr Mikulčík	**Josef Šňupík**	**Lenka Kneslová**	**Radomír Štipčák**	**Miroslav Smuda**
Ředitel/Vedoucí výroby ROSTRA Stamping	Vedoucí obchodního úseku	Vedoucí ekonomického úseku	Vedoucí výroby ROSTRA Tools	Vedoucí úseku kvality