BEZPEČNOSTNÍ STRATEGIE SPOLEČNOSTI MEDUNA VAKUOVÁ KALÍRNA
2026–2028

1. STRATEGIE SPOLEČNOSTI

Společnost MEDUNA VAKUOVÁ KALÍRNA se zavazuje k systematickému a dlouhodobému zajišťování bezpečnosti informací, technologií a procesů jako nedílné součásti řízení společnosti.

Společnost se rozhodla:

- udržovat, provozovat a neustále zlepšovat systém řízení bezpečnosti informací (ISMS) v souladu s normou ČSN EN ISO/IEC 27001:2023 v celé společnosti,
- podporovat integrovat bezpečnost informací do všech klíčových procesů řízení, výroby a poskytování služeb,
- systematicky řídit rizika v oblasti informační a kybernetické bezpečnosti,
- chránit informace, technologie a know-how společnosti před hrozbami v oblasti kybernetické, fyzické i organizační bezpečnosti,
- zajišťovat kontinuitu kritických činností společnosti a odolnost vůči mimořádným událostem,
- plnit všechny relevantní právní, smluvní a regulatorní požadavky, zejména v oblasti kybernetické bezpečnosti, ochrany osobních údajů a ochrany informací.

Prostřednictvím ISMS společnost usiluje zejména o:

- ochranu důvěrnosti, integrity a dostupnosti informací,
- minimalizaci rizik bezpečnostních incidentů a jejich dopadů,
- zvyšování odolnosti společnosti vůči kybernetickým hrozbám a provozním výpadkům,
- posilování důvěry zákazníků, obchodních partnerů a dalších zainteresovaných stran.

2. ZÁVAZEK VEDENÍ

Vedení společnosti vyjadřuje schválením této strategie svůj závazek:

- aktivně podporovat ISMS jako nedílnou součást systému řízení společnosti,
- zajišťovat dostupnost potřebných zdrojů (personálních, finančních, technických a organizačních),
- stanovovat jasné role, odpovědnosti a pravomoci v oblasti bezpečnosti informací,
- podporovat kulturu bezpečnosti a odpovědnosti na všech úrovních společnosti,
- pravidelně přezkoumávat výkonnost ISMS a jeho soulad s cíli společnosti,
- podporovat neustálé zlepšování bezpečnostních opatření na základě analýzy rizik, incidentů, auditů a změn v prostředí společnosti.

3. CÍLE ISMS

Základními cíli ISMS jsou:

- Důvěrnost – zabránit neoprávněnému přístupu k informacím,

- Integrita – zajistit správnost, úplnost a ochranu před neoprávněnými změnami,
- Dostupnost – zajistit dostupnost informací a systémů oprávněným uživatelům v požadovaném čase.

Tyto obecné cíle jsou rozpracovány do konkrétních měřitelných cílů, zejména v oblastech:

- řízení rizik a souladu s právními požadavky a dalšími relevantními normativními požadavky,
- řízení dodavatelů a třetích stran,
- ochrany IT a OT infrastruktury a výrobních technologií,
- připravenosti na incidenty a krizové situace,
- zvyšování bezpečnostního povědomí zaměstnanců.

4. ZAPOJENÍ VŠECH PRACOVNÍKŮ SPOLEČNOSTI

Naplnění této strategie vyžaduje aktivní zapojení všech zaměstnanců a spolupracujících osob a jejich odpovědné chování v oblasti ochrany informací.

Každý zaměstnanec a spolupracující osoba je povinen:

- chránit informace v souladu s jejich hodnotou, citlivostí a určením,
- dodržovat bezpečnostní politiky, směrnice a postupy společnosti,
- používat informační a komunikační technologie bezpečným a odpovědným způsobem,
- neprodleně hlásit bezpečnostní události, slabiny a incidenty,
- účastnit se povinných školení v oblasti kybernetické a informační bezpečnosti a přispívat ke zvyšování bezpečnostního povědomí.

5. PLATNOST STRATEGIE

Tato strategie je platná pro období 2026–2028 a je přezkoumávána při významné změně vnitřního nebo vnějšího prostředí společnosti nebo na základě rozhodnutí vedení společnosti.

Vytvořil: Viktor Novák
Manažer bezpečnosti informací

Dne 7.1.2026 v Pardubicích

Schválil: Vendula Nováková
Jednatelka společnosti

Dne 7.1.2026 v Pardubicích