



# Politika ISMS (Information Security Management System)

## Prohlášení managementu

Vedení společnosti BMT Medical Technology s.r.o. (dále jen BMT) vyhláší zásady bezpečnosti informací. Tato politika je závazná pro všechny zaměstnance společnosti, kterých se systém řízení bezpečnosti informací týká a spolupracující organizace.

Záměrem vedení BMT je udržovat přiměřenou ochranu informačních aktiv v souladu se zákony a jinými právními předpisy ČR a EU, a to i v případech, kdy byla odpovědnost za zpracování informací přenesena na spolupracující organizace.

## Cíle bezpečnosti informací

Naším cílem je zajistit důvěrnost, integritu a dostupnost všech vlastních a zákaznických dat pro bezproblémové zajištění našich podnikatelských aktivit a zajistit provoz kritické informační infrastruktury. K prosazování této politiky je ve společnosti zaveden a rozvíjen systém managementu bezpečnosti informací dle ISO/IEC 27001.

### Zavazujeme se:

- dodržovat a naplňovat legislativní předpisy pro oblast bezpečnosti informací a kybernetické bezpečnosti,
- zajišťovat dostupnost informací v čase a místě dle potřeb společnosti, ale pouze těm, kteří je potřebují pro svoji pracovní činnost, čímž je zachovávána důvěrnost informací dle stanovených kategorií – veřejné, interní, důvěrné, osobní,
- řídit integritu a životní cyklus informací od okamžiku jejich vzniku, předávání, užívání až po likvidaci,
- vzdělávat a rozvíjet naše zaměstnance, dodavatele a partnery v oblasti bezpečnosti informací a kybernetické bezpečnosti,
- porušení pravidel informační a kybernetické bezpečnosti je považováno za hrubé porušení interních předpisů a smluvních vztahů

### Ve vztahu k dodavatelům se zavazujeme:

- zajistit ochranu aktiv organizace, ke kterým mají dodavatele přístup,
- požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům organizace odsouhlasit s dodavatelem a řádně zadokumentovat,
- požadavky relevantní bezpečnosti informací ustavit a odsouhlasit s každým dodavatelem, který může přistupovat k informacím organizace, zpracovává je, ukládá nebo zajišťuje prvky IT infrastruktury či prvky kritické informační infrastruktury,
- v dohodách s dodavatelem zahrnout požadavky na rizika bezpečnosti informací a kybernetické bezpečnosti spojená s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií,
- udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami

### Dále:

- společnost pravidelně monitoruje a přezkoumává dodávky služeb dodavatelů,
- změny v poskytování služeb dodavatelem, včetně změn v udržování a zlepšování existujících politik, postupů a opatření bezpečnosti informací, řídíme s ohledem na kritičnost informací, systémů a procesů organizace, které jsou součástí těchto změn, a s ohledem na opakované posouzení rizik.

## Závazek ke splnění aplikovatelných požadavků

Touto politikou deklarujeme všem obchodním partnerům, zaměstnancům i majitelům, veřejné a státní správě a široké veřejnosti schopnost celé společnosti efektivně chránit informace, prvky kritické infrastruktury, hmotný i nehmotný majetek vlastní i nám svěřený v souladu s legislativními požadavky s platnou legislativou České republiky i Evropské unie, mezinárodními smlouvami a jinými požadavky na ochranu bezpečnosti informací.

## Závazek k neustálému zlepšování

### Zavazujeme se:

- stanovovat přijímaná bezpečnostní opatření na principu posouzení závažnosti vyhodnocených rizik, jejich dopadů a ekonomické náročnosti opatření,
- zvyšovat účinnost našeho systému managementu bezpečnosti informací pravidelným monitorováním, přehodnocováním rizik, řízením bezpečnostních událostí a incidentů prostřednictvím nápravných a preventivních opatření