

## Politika integrovaného systému

dle ČSN ISO/IEC 27001:2014 a ČSN ISO/IEC 20000-1:2019



Vedení organizace **ManpowerGroup s.r.o.**, jejímž jedním z hlavních předmětů činnosti je poskytování IT služeb, se zavazuje k dalšímu rozvoji organizace, neustálému zlepšování úrovně kvality služeb k všestrannému uspokojování očekávaných i předpokládaných potřeb zákazníků a naplňování požadavků právních předpisů.

Tato politika má za cíl informovat zákazníky a partnery společnosti i veřejnost o trvalém zájmu chránit všechna informační aktiva a aktiva využívaná na jejich zpracování vůči externím i interním hrozbám, jejich zneužití, prozrazení nebo zničení.

Základním smyslem systému informační bezpečnosti je zabezpečit kontinuální integritu, dostupnost a důvěrnost datových a jiných aktiv. Vedení společnosti si je vědomo odpovědnosti za neustálé zvyšování jistoty vlastních aktiv i aktiv našich klientů a ostatních partnerů a produktů poskytovaných stávajícím i novým zákazníkům společnosti s cílem maximálního uspokojení potřeb svých zákazníků. Proto se rozhodlo pro zavedení dokumentovaného systému managementu informační bezpečnosti podle modelu procesně orientovaného systému ČSN ISO/IEC 27001:2014 a ČSN ISO/IEC 20000-1:2019.

V rámci procesu zlepšování ISMS, vedení firmy bude věnovat trvalou pozornost následujícím oblastem:

- Zabezpečit soulad našeho ISMS s obchodními požadavky našich zákazníků a partnerů i se zákony, vyhláškami a všemi relevantními předpisy. Vyhnout se porušením jakýchkoliv zákonných, statutárních, regulačních nebo smluvních závazků a jakýchkoliv bezpečnostních požadavků. Zejména dodržovat zásady vycházející z obecného nařízení o ochraně osobních údajů GDPR.
- Řídit rozvoj informační bezpečnosti uvnitř společnosti i na rozhraních s našimi zákazníky i partnery.
- Dosáhnout, udržovat a zlepšovat přiměřenou ochranu aktiv společnosti i našich zákazníků a partnerů. Proto je zkoumána a vyhodnocována situace z hlediska rizik (viz analýza bezpečnostních rizik), kde vedení rozhodne o rozdělení na akceptovatelná a neakceptovatelná a pro ně následně zavádí opatření.
- Trvale zajistit, aby bezpečnost a kompatibilita byly integrální součástí našich informačních produktů.

V Praze, dne 1. 7. 2020

Ing. Petr Matějka