MGVIVA a.s., Malešická 2251/51**,** Praha 3, 130 00
Tel.: +420 225 001 532, e-mail: mgviva@mgviva.cz

Politika bezpečnosti informací společnosti MGVIVA a.s.

Kontext a účel

Společnost MGVIVA a.s. působí jako distributor, dovozce a servisní organizace zdravotnických prostředků a gastronomické technologie. Služby a dodávky směřují převážně k veřejným zadavatelům, což klade vysoké nároky na důvěryhodnost, transparentnost a ochranu informací. Vzhledem k charakteru svých činností si společnost plně uvědomuje rizika spojená s únikem, zneužitím nebo narušením důvěrnosti, dostupnosti a integrity informací. Zavazuje se proto k jejich aktivnímu řízení prostřednictvím systému řízení informační bezpečnosti (ISMS), který je součástí integrovaného systému managementu. Cílem této politiky je chránit informační aktiva, systémy a data společnosti, zajistit provozní kontinuitu, důvěru zákazníků a plnění smluvních i zákonných povinností.

Rozsah působnosti

Politika se vztahuje na všechny zaměstnance, externí spolupracovníky, dodavatele a další osoby, které přistupují k informačním systémům nebo datům společnosti. Je závazná pro všechna zařízení, systémy, aplikace a komunikační kanály využívané v rámci činností společnosti. Uplatňuje se ve všech lokalitách, kde společnost působí, a na všech úrovních řízení.

Závazek vedení

Vrcholové vedení společnosti se zavazuje poskytovat potřebné zdroje pro fungování ISMS, podporovat kulturu bezpečnosti napříč organizací a pravidelně přezkoumávat a zlepšovat systém. Vedení aktivně podporuje dodržování této politiky, stanovuje cíle informační bezpečnosti a zajišťuje, že odpovědnosti jsou jasně definovány, komunikovány a uplatňovány v praxi.

Role a odpovědnosti

Společnost stanovuje jasné role a odpovědnosti v oblasti informační bezpečnosti. Manažer integrovaného systému odpovídá za zavedení a udržování ISMS. Manažer kybernetické bezpečnosti metodicky vede bezpečnostní fórum, navrhuje technická řešení a provádí audity. Správce IT zajišťuje provozní bezpečnost, správu přístupů, zálohování a monitoring. Interní auditor kontroluje dodržování směrnic a navrhuje nápravná opatření. Compliance manažer sleduje soulad s legislativou a interními pravidly. Vlastníci aktiv odpovídají za ochranu přidělených informačních aktiv.

Řízení rizik a bezpečnostní opatření

Společnost identifikuje hrozby, zranitelnosti a rizika, a přijímá odpovídající technická a organizační opatření. Mezi klíčové oblasti patří bezpečnost hesel, šifrování dat, ochrana mobilních zařízení, pravidla pro používání externích médií, fyzická

bezpečnost IT aktiv a pravidla pro vzdálené připojování. Opatření jsou navržena tak, aby odpovídala úrovni rizika a významu chráněných informací.

Ochrana elektronické komunikace

Firemní e-mailové účty smí být používány výhradně pro pracovní účely. Používání soukromých e-mailů na firemních zařízeních je zakázáno. Při práci s elektronickou poštou je nutné dbát zvýšené opatrnosti, zejména při otevírání příloh a odkazů. V případě podezření na bezpečnostní incident je nutné neprodleně kontaktovat Správce IT nebo Manažera kybernetické bezpečnosti.

Zálohování a obnova dat

Data jsou pravidelně zálohována na centrálních úložištích. Uživatelé jsou povinni ukládat chráněná data výhradně na síťové disky nebo do prostředí M365. Obnova dat probíhá dle definovaných postupů a za asistence Správce IT. Zálohovací procesy jsou pravidelně testovány a dokumentovány.

Dodržování právních a smluvních požadavků

Společnost dodržuje všechny relevantní právní, smluvní a regulační požadavky v oblasti informační bezpečnosti. ISMS je navržen tak, aby podporoval soulad s těmito požadavky a umožňoval jejich prokazatelné plnění. Všichni zaměstnanci jsou povinni jednat v souladu s platnými předpisy a interními směrnicemi.

Školení a povědomí

Společnost podporuje vzdělávání zaměstnanců v oblasti informační bezpečnosti. Pravidelná školení zvyšují povědomí o rizicích, pravidlech a správném chování při práci s informacemi. Noví zaměstnanci absolvují vstupní školení, stávající jsou pravidelně proškolováni. Všichni zaměstnanci jsou povinni se školení účastnit a aktivně přispívat k bezpečnostní kultuře.

Neustálé zlepšování

ISMS je pravidelně přezkoumáván, aktualizován a zlepšován na základě interních auditů, zpětné vazby a vývoje hrozeb. Společnost vítá návrhy na zlepšení systému od zaměstnanců i třetích stran. Výsledky přezkoumání slouží jako podklad pro stanovení nových cílů a priorit v oblasti informační bezpečnosti.

V Praze, dne 24.11.2025

Schváleno vrcholovým vedením společnosti MGVIVA a.s.