OBSAH

Rozdeľovník

Dokument v elektronickej forme:	Všetci pracovníci

Činnosť	**Meno a priezvisko**	**Funkcia**	**Podpis**	
Vypracoval	Marek Olexa	Manager Q/E/IS/BC	Marek Olexa Digitally signed by Marek Olexa Date: 2023.10.10 16:06:47 +02'00'	
Preveril	Vladimír Hutta	Chief Financial Officer	Digitally signed by Vladimír Hutta Date: 2023.10.10 16:12:03 +02'00'	
Schválil	Peter Jamrich	Company Director	Peter Jamrich Digitally signed by Peter Jamrich Date: 2023.10.10 16:31:13 +02'00'	

1. RIADENIE INFORMAČNEJ BEZPEČNOSTI

Vedenie spoločnosti MicroStep - HDO s.r.o. sa zaväzuje chrániť **dôvernosť, integritu a dostupnosť** informačných aktív v rámci celej organizácie. Dodržiavanie tohto záväzku je dlhodobo nutné pre získanie a udržanie konkurenčnej výhody, ziskovosti, súladu s legislatívnymi a zmluvnými záväzkami a imidžu spoľahlivej a dôveryhodnej firmy.

Spoločnosť MicroStep - HDO s.r.o. zaviedla plány kontinuity pre poskytovanie služieb, ktoré sú kritické pre našich zákazníkov. Plány kontinuity udržiavame, aktívne testujeme a na základe získaných výsledkov sa zaväzujeme ich priebežne vylepšovať.

Za týmto účelom spoločnosť zaviedla a prevádzkuje systém riadenia informačnej bezpečnosti (ISMS, Information Security Management System) podľa normy **ISO/IEC 27001:2013** a systém riadenia kontinuity podnikania (BCMS, Business continuity management systems) podľa normy **ISO 22301:2019.** Systém riadenia pokrýva všetky priestory v sídle spoločnosti v Bratislave, všetky informačné systémy a ostatné informačné aktíva. Hlavný dôraz je pritom kladený na ochranu aktív súvisiacich s:

- dodržiavaním zmluvných a legislatívnych záväzkov,
- ochranou osobných údajov a súkromia,
- ochranou duševného vlastníctva,
- zabezpečením dát organizácie,
- riadením kontinuity v prípade havárií, napadnutia a komplexných výpadkov.

Vedenie spoločnosti MicroStep - HDO s.r.o. si je vedomé, že samotné technické opatrenia nepostačujú na minimalizovanie všetkých existujúcich hrozieb, a preto bude aktívne formovať a zlepšovať **bezpečnostné povedomie** zamestnancov a pravidelne testovať postupy zotavenia po závažných výpadkoch.

Pre účinné riadenie informačnej bezpečnosti a kontinuity podnikania je menovaná **Rada informačnej bezpečnosti**. V jej čele stojí Manažér Q/E/IS/BC. Pre závažné udalosti narúšajúce činnosť spoločnosti sú vytvorené **havarijné tímy.** Celý systém kontinuity podnikania je riadený Manažérom systému kontinuity podnikania.

Na dôkaz dodržiavania požiadaviek spomínaných noriem sa spoločnosť podrobuje pravidelným externým auditom vykonávaným akreditovaným certifikačným orgánom.

Všetci zamestnanci musia konať v súlade s touto politikou a postupmi vyplývajúcimi zo zavedeného systému riadenia informačnej bezpečnosti. Spoločnosť zaviedla jasné a transparentné disciplinárne opatrenia pre prípady porušovania schválených bezpečnostných opatrení. Rovnako tak **určené tretie strany** musia dodržiavať bezpečnostné záväzky vyplývajúce z požiadaviek systému riadenia informačnej bezpečnosti, ktoré sú premietnuté do vzájomných zmlúv.

Táto politika je prehodnocovaná vedením spoločnosti minimálne 1x ročne.

1.1. HODNOTENIE BEZPEČNOSTNÝCH RIZÍK

Zachovanie bezpečnosti informačných aktív je v súlade s obchodnými cieľmi spoločnosti. Systém riadenia informačnej bezpečnosti slúži ako nástroj na znižovanie súvisiacich rizík na akceptovateľnú úroveň. **Posudzovanie rizík je základom účinného fungovania systému a podkladom pre účelné vynakladanie zdrojov.** Vykonáva sa podľa potreby, no najmenej 1x ročne.

Výsledky posúdenia rizík sú predkladané vedeniu spoločnosti, ktoré rozhoduje o kritériách pre akceptovanie rizík a schvaľuje zostatkové riziká.

1.2. ZVLÁDANIE BEZPEČNOSTNÝCH INCIDENTOV A HAVARIJNÝCH STAVOV

Kvôli schopnosti správnej reakcie na neželané bezpečnostné udalosti je zavedený **systém sledovania a ohlasovania bezpečnostných incidentov**. Všetci zamestnanci sú poučovaní o tom, ako reagovať a koho informovať, ak zaznamenajú podozrivú aktivitu.

Riešenie havarijných situácií a plánov kontinuity je testované aspoň 1x ročne. Získané skúsenosti musia byť zapracované do plánov kontinuity.

1.3. HODNOTENIE A ZLEPŠOVANIE MANAŽÉRSKYCH SYSTÉMOV

Na vyhodnocovanie účinnosti systému riadenia informačnej bezpečnosti a systému riadenia kontinuity podnikania sú zavedené postupy monitorovania a interných auditov. Účinnosť manažérskych systémov je aspoň 1x ročne vyhodnocovaná vedením spoločnosti.

2. ZÁVEREČNÉ USTANOVENIA

Všetci pracovníci sú povinní sa s touto politikou, jej zmenami a doplnkami preukázateľne oboznámiť.