Bezpečnostní politika pro významné dodavatele společnosti Apatyka servis, s.r.o.

Zpracoval:	Manažer kybernetické bezpečnosti (J. Mináč) 23.11.2026

1. Účel dokumentu

Společnost Apatyka servis, s.r.o. (dále jen „Apatyka“) provozuje systém řízení bezpečnosti informací (ISMS) v souladu s požadavky normy ISO/IEC 27001, zákona o kybernetické bezpečnosti a souvisejících regulatorních požadavků.

Účelem této politiky je definovat základní principy a očekávání společnosti Apatyka v oblasti informační a kybernetické bezpečnosti vůči významným dodavatelům, kteří poskytují služby, produkty nebo podporu související s provozem informačních systémů, zpracováním informací nebo poskytováním regulovaných služeb společnosti Apatyka.

2. Závazek k informační a kybernetické bezpečnosti

Apatyka očekává, že významní dodavatelé budou při poskytování svých služeb uplatňovat přiměřená organizační, procesní a technická opatření k ochraně informací a souvisejících aktiv.

Dodavatelé by zejména měli:

- uplatňovat principy ochrany důvěrnosti, integrity a dostupnosti informací,
- průběžně identifikovat a řídit bezpečnostní rizika související s poskytovanými službami,
- podporovat kontinuální zvyšování úrovně informační a kybernetické bezpečnosti,
- zajistit odpovídající řízení bezpečnosti v rámci svých interních procesů a organizace,
- spolupracovat se společností Apatyka při řešení bezpečnostních otázek souvisejících s poskytovanými službami.

3. Ochrana informací a informačních aktiv

Dodavatel je povinen zajistit odpovídající ochranu informací, které získá, zpracovává nebo jiným způsobem využívá v souvislosti s poskytováním služeb společnosti Apatyka.

Dodavatel zejména:

- využívá informace pouze k účelům vyplývajícím ze smluvního vztahu,
- omezuje přístup k informacím výhradně na oprávněné osoby,
- zavádí opatření proti neoprávněnému přístupu, zveřejnění, změně, ztrátě nebo zničení informací,
- respektuje požadavky společnosti Apatyka na klasifikaci a ochranu informací,
- přiměřeně chrání informační a technická aktiva využívaná při poskytování služeb.

4. Ochrana osobních údajů

V případech, kdy dodavatel zpracovává osobní údaje, je povinen zajistit jejich ochranu v souladu s platnými právními předpisy, zejména nařízením Evropského parlamentu a Rady (EU) 2016/679 (GDPR).

Dodavatel zejména:

- zpracovává osobní údaje pouze v rozsahu nezbytném pro stanovený účel,
- omezuje přístup k osobním údajům pouze na oprávněné osoby,
- přijímá odpovídající technická a organizační opatření k jejich ochraně,
- podporuje naplňování práv subjektů údajů.

5. Personální bezpečnost

Dodavatel zajistí, aby osoby podílející se na poskytování služeb společnosti Apatyka byly přiměřeně poučeny o bezpečnostních požadavcích a povinnostech vyplývajících z jejich pracovní činnosti.

Očekává se zejména, že:

- pracovníci budou seznámeni s relevantními bezpečnostními pravidly,
- budou vázáni odpovídající povinností mlčenlivosti,
- budou disponovat potřebnou kvalifikací a znalostmi pro vykonávanou činnost,
- budou pravidelně vzděláváni v oblasti informační a kybernetické bezpečnosti.

6. Řízení aktiv a rizik

Dodavatel by měl uplatňovat systematický přístup k identifikaci, hodnocení a řízení rizik souvisejících s poskytovanými službami.

Součástí tohoto přístupu by mělo být zejména:

- průběžné vyhodnocování relevantních hrozeb a zranitelností,
- zohledňování bezpečnostních rizik při provozu a rozvoji poskytovaných služeb,
- přijímání opatření odpovídajících významu identifikovaných rizik,
- pravidelné přezkoumávání účinnosti zavedených opatření.

7. Dodržování právních a regulatorních požadavků

Dodavatel je odpovědný za dodržování právních, regulatorních a smluvních požadavků vztahujících se k poskytovaným službám.

Očekává se zejména soulad s:

- právními předpisy upravujícími ochranu osobních údajů,
- právními předpisy v oblasti kybernetické bezpečnosti,

- regulatorními požadavky vztahujícími se k poskytovanému plnění,
- interními pravidly a požadavky společnosti Apatyka, které byly dodavateli zpřístupněny.

8. Spolupráce v oblasti bezpečnosti

Apatyka považuje bezpečnost za sdílenou odpovědnost mezi objednatelem a dodavatelem.

Významní dodavatelé by proto měli podporovat otevřenou, transparentní a profesionální spolupráci v oblasti informační a kybernetické bezpečnosti, aktivně přispívat k identifikaci a snižování bezpečnostních rizik a napomáhat dosahování bezpečnostních cílů společnosti Apatyka.

9. Závěrečné ustanovení

Tato politika stanovuje základní bezpečnostní očekávání společnosti Apatyka vůči významným dodavatelům. Konkrétní bezpečnostní povinnosti, odpovědnosti, kontrolní mechanismy a oznamovací povinnosti jsou upraveny příslušnými smlouvami, dodatky a související smluvní dokumentací mezi společností Apatyka a konkrétním dodavatelem.