

PŘÍLOHA 1: POLITIKA SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ – MINISTERSTVO PRO CERTIFIKACI SENZORŮ

Verze dokumentu			
datum	verze	změněno	provedená změna
2.2.2026	1.0	Manažer KB	Vytvoření dokumentu
28.2.2026	1.0	Výbor pro řízení KB	Schválení dokumentu
18. 3. 2026	2.0	Manažer KB	Přezkoumání Politiky systému řízení bezpečnosti informací
5. 4. 2026	2.0	Výbor pro řízení KB	Schválení aktualizované verze dokumentu

1 Účel

Účelem této politiky je deklarovat a schválit vedením Ministerstva pro certifikaci senzorů (dále jen „ministerstvo“) politiku systému řízení bezpečnosti informací (dále jen „ISMS“), strategické cíle ISMS, rozsah řízení kybernetické bezpečnosti (dále jen „KB“) a další pravidla a postupy související s řízením KB.

Politika ISMS musí být přezkoumána manažerem KB minimálně 1x za rok a při významné změně. I v případě, že nedojde k žádným změnám, musí být u verze uvedeno datum přezkoumání.

2 Závazek vedení

Vedení ministerstva se zavazuje ke vzniku, řízení, kontrole a podpoře uceleného a funkčního ISMS. Dále se ministerstvo zavazuje k vytvoření podmínek pro získání lidských, technických a finančních zdrojů, které jsou nezbytné pro ustavení, fungování a neustálé zlepšování ISMS.

3 Cíle, principy a potřeby systému řízení bezpečnosti informací

Ministerstvo si stanovilo následující strategické cíle:

- Zajištění souladu s právními předpisy
- Zajištění jednotné ochrany informací podle požadavků legislativy u regulovaných služeb
- Zajištění odpovídajících zdrojů (personálních, technických i finančních) pro oblast bezpečnosti informací
- Implementace bezpečnostních technologií a jejich průběžná aktualizace a modernizace
- Zajištění schopnosti zvládnutí kybernetických bezpečnostních událostí a incidentů
- Zajištění adekvátní úrovně důvěrnosti, integrity a dostupnosti
- Formalizace procesů a postupů
- Stanovení odpovědností
- Zvýšení úrovně bezpečnostního povědomí zaměstnanců

Měřitelné cíle ISMS:

- V rámci rozsahu řízení KB regulované služby zajistit soulad s legislativními požadavky alespoň na 80 %
- Pomocí školení v oblasti KB zajistit, že alespoň 90 % kybernetických bezpečnostních událostí a incidentů bude nahlášeno v ServiceDesku
- Absolvování vstupních a pravidelných školení v oblasti KB alespoň u 90 % zaměstnanců ministerstva

4 Rozsah řízení kybernetické bezpečnosti

Ministerstvo stanovilo rozsah řízení KB pro všechna aktiva s výjimkou těch, která souvisejí s provozem dětské skupiny. Tento proces probíhal ve třech krocích:

- Nejprve byla určena všechna primární aktiva.
- Následně bylo vyhodnoceno, zda tato aktiva souvisejí s poskytováním regulované služby, přičemž bylo rozhodnuto, že aktiva týkající se provozu dětské skupiny s regulovanou službou nesouvisejí.
- Ve třetím kroku byla na základě definovaného rozsahu určena odpovídající podpůrná aktiva.

Tabulka 1: Modelový příklad posouzení souvislosti primárních aktiv s regulovanou službou

Souvisí s poskytováním regulované služby	Nesouvisí s poskytováním regulované služby
S1 – Služba certifikace senzorů	S2 – Provoz dětské skupiny
P1 – Seznam certifikovaných senzorů	P5 – Informace o přítomnosti
P2 – Rozhodnutí	P6 – Personální údaje dětí a zákonných zástupců
P3 – Žádosti, technická dokumentace	P7 – Provozní dokumentace
P4 – Informace o průběhu certifikace	...
...	

Klíčovou činností ministerstva, která je součástí rozsahu řízení KB, je certifikace senzorů a ověřování, zda předložené senzory splňují všechny požadavky na ně kladené a vyhovujícím zařízením uděluje tříletou certifikaci. Kromě kontroly dokumentace ministerstvo provádí také testování ve vlastní laboratoři.

Určený rozsah řízení KB zahrnuje:

- Fyzické aspekty rozsahu řízení KB
 - **Fyzický perimetr** zahrnuje všechny objekty a prostory, v nichž jsou umístěna nebo spravována aktiva služby certifikace senzorů, tedy jak prostory ve vlastnictví organizace, tak i ty, které nevlastní, ale má je pronajaté. Tyto objekty se nacházejí na následujících adresách:
 - Smyšlená 1, Praha 1, 123 45,
 - Smyšlená 2, Praha 1, 123 45,
 - Smyšlená 3, Praha 1, 123 45.
- Organizační a personální aspekty rozsahu řízení KB
- **Všichni zaměstnanci organizace a další osoby**, které se podílejí na poskytování regulované služby ministerstva.
 - **Dodavatelé (včetně subdodavatelů)**, kteří participují na dodávkách primárních a podpůrných aktiv i ve smyslu poskytované regulované služby.
- Technologické aspekty rozsahu řízení KB
 - **Primární a podpůrná aktiva v rámci organizace**, která spadají do určeného rozsahu řízení KB.
 - **Primární a podpůrná aktiva spravovaná nebo provozovaná dodavateli**, která spadají do určeného rozsahu řízení KB.

Konkrétní výčet primárních a podpůrných aktiv lze nalézt v katalogu aktiv (viz *Příloha 6: Vzorové hodnocení aktiv a rizik*). Rozsah řízení KB je také určen topologií komunikační sítě.

5 Pravidla a postupy pro pravidelné vyhodnocení účinnosti systému řízení bezpečnosti informací

Pravidelné vyhodnocení účinnosti ISMS ministerstva probíhá každý rok a obsahuje hodnocení současného stavu, trendů a příležitostí pro další rozvoj, eventuálně nutnost případných změn tak, aby byla zajištěna trvalá vhodnost, přiměřenost a efektivnost systému, včetně příležitostí pro zlepšení. Vyhodnocení účinnosti ISMS provádí manažer KB v součinnosti s dalšími bezpečnostními rolemi a zainteresovanými stranami a následně je zpráva z přezkoumání ISMS projednána na výboru pro řízení KB.

5.1 Vstupy do vyhodnocení účinnosti ISMS

- Vyhodnocení opatření z předchozího přezkoumání ISMS
- Posouzené významné změny a okolnosti, které mohou mít vliv na ISMS
- Zpětná vazba o výkonnosti ISMS
 - Neshody a nápravná opatření
 - Výsledky monitorování a měření
 - Výsledky předchozích auditů KB
 - Naplnění cílů ISMS
- Výsledky hodnocení rizik, včetně revize hodnocení rizik, a stav plnění plánu zvládání rizik
- Výstupy ze skenování zranitelností a penetračního testování
- Přehled kybernetických bezpečnostních událostí a incidentů za uplynulé období
- Vyhodnocení plánu vzdělávání v oblasti KB
- GAP analýza (viz Průvodce řízením aktiv a rizik dle vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností – kapitola 5.4 Katalog bezpečnostních opatření)

5.2 Výstupy z přezkoumání ISMS

- Určování možností pro neustálé zlepšování
- Doporučení potřebných rozhodnutí, stanovení nápravných opatření a osob zajišťujících výkon jednotlivých činností

6 Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací

Veškerá nápravná opatření vychází ze zprávy z přezkoumání ISMS. Tato nápravná opatření jsou projednána výborem pro řízení KB. K jednotlivým nápravným opatřením jsou stanoveny osoby odpovědné za zavedení nápravných opatření a dodržení termínu zavedení nápravného opatření.

Nápravná opatření jsou čtvrtletně sledována v rámci výboru pro řízení KB.