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

| Verze dokumentu | | | |
|---|---|---|---|
| **Datum** | **Verze** | **Změněno** | **Provedená změna** |
| 3.9.2020 | 1.0 | Manažer kybernetické bezpečnosti | Vytvoření dokumentu |
| 1.10.2020 | 1.0 | Výbor KB | Schválení dokumentu |
| 18. 9. 2021 | 2.0 | Manažer kybernetické bezpečnosti | Přezkoumání Politiky systému řízení bezpečnosti informací |
| 1. 10. 2021 | 2.0 | Výbor KB | Schválení aktualizované verze dokumentu |

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

Politika systému řízení bezpečnosti informací musí být přezkoumána manažerem kybernetické bezpečnosti minimálně 1x za dva roky. I v případě, že nedojde k žádným změnám, musí být u verze uvedeno datum přezkoumání.

**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 neustálého zlepšování ISMS.

**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 kritických prvků infrastruktury a aplikací
- Zajištění odpovídajících zdrojů (personálních, technických i finančních) pro oblast bezpečnosti informací
- Implementace bezpečnostních technologií a jejich průběžná aktualizace a modernizace
- Zajištění schopnosti zvládání bezpečnostních událostí a incidentů
- Zajištění adekvátní úrovně důvěrnosti, integrity a dostupnosti
- Formalizace procesů a postupů
- Stanovení zodpovědností
- Zvýšení úrovně bezpečnostního povědomí zaměstnanců

Měřitelné cíle systému řízení bezpečnosti informací:

- V rámci určených systémů zajistit soulad s legislativními požadavky alespoň na 80 %
- Pomocí školení v oblasti kybernetické bezpečnosti zajistit, že alespoň 90 % kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů bude nahlášeno v ServiceDesku

**Rozsah a hranice systému řízení bezpečnosti informací**

Ministerstvo se rozhodlo určit rozsah ISMS pouze pro dílčí službu certifikace senzorů a příslušný systém: agendový (certifikační) systém. Vše, co je níže vyjmenováno, se týká pouze tohoto agendového systému. Klíčovou činností, na kterou je i stanoven rozsah ISMS ministerstva, 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.

Ministerstvo se rozhodlo určit rozsah ISMS pouze pro dílčí agendový (certifikační) systém a rozsah ISMS zahrnuje:

- Fyzické aspekty rozsahu
    - **Fyzický perimetr**, který pokrývá všechny objekty a prostory, ve kterých je využíván a provozován agendový systém, tedy prostory, které jsou ve vlastnictví této organizace, ale i prostory, které nevlastní a má v nájmu. Tyto objekty se nacházejí na těchto adresách:
        - Smyšlená 1, 123 45 Praha 1,
        - Smyšlená 2, 123 45 Praha 1,
        - Smyšlená 3, 123 45 Praha 1.
- Organizační a personální aspekty rozsahu
    - **Všichni zaměstnanci organizace a další osoby**, které využívají agendový systém k výkonu činnosti ministerstva
    - **Dodavatelé (včetně subdodavatelů)**, kteří participují na dodávkách primárních a podpůrných aktiv i ve smyslu poskytovaných služeb
- Technologické aspekty rozsahu
    - **Primární a podpůrná aktiva v rámci organizace**, která podporují službu certifikace a agendový systém
    - **Primární a podpůrná aktiva spravovaná nebo provozovaná dodavateli**, která podporují službu certifikace a agendový systém

Konkrétní výčet primárních a podpůrných aktiv lze nalézt v katalogu aktiv (viz Příloha 6: Vzorové hodnocení aktiv a rizik). Rozsah ISMS agendového systému je také určen topologií systému.

**Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací**

Pravidelné přezkoumání 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. Přezkoumání provádí manažer kybernetické bezpečnosti v součinnosti s dalšími bezpečnostními rolemi a zainteresovanými stranami a následně je zpráva z přezkoumání ISMS projednána na výboru KB.

Vstupy do přezkoumání ISMS:

- Vyhodnocení opatření z předchozího přezkoumání ISMS
- Identifikace změn a okolností, 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 a stav plnění plánu zvládání rizik
- Výstupy ze skenování zranitelností a penetračního testování

- Přehled kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů za uplynulé období
- Vyhodnocení plánu vzdělávání v oblasti KB
- GAP analýza (viz Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti kapitola 5.4)

Výstupy z přezkoumání

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

**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 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 KB.