Ceny Ministerstva vnitra za kvalitu a inovaci ve veřejné správě

ročník 2010

ZÁVĚREČNÁ ZPRÁVA Z ŘEŠENÍ

☐ **bronzového stupně ceny**

X **stříbrného stupně ceny**

☐ **inovace**

(zatrhněte cenu, o jakou soutěžíte)

1. Název řešení:

Implementace systému bezpečnosti informací (ISMS) u Městského úřadu Žamberk.
(ČSN ISO/IEC 27001 a ČSN ISO/IEC 17799)

2. Autor zprávy:

Jméno: Ing. Vladimír Fikejs
Funkce: vedoucí odboru obrany a krizového řízení, představitel vedení pro ISMS
Organizace: Městský úřad Žamberk, Masarykovo nám. 166, 564 01 Žamberk
Telefon: 465 670 218
E-mail: v.fikejs@muzbk.cz

3. Organizace, kde bylo řešení aplikováno:

Městský úřad Žamberk

4. Popis řešení

4.1 Podstata řešení:

Postup: Přijetí ustanovení ČSN ISO/IEC 27001 a ČSN ISO/IEC 17799, vytyčení základního předpisu Politiky bezpečnosti informací, podpora ze strany vedení městského úřadu a přijetí zásad bezpečnosti informací všemi zaměstnanci úřadu. Toto úsilí bylo završeno certifikačním auditem a udělením certifikátu ISO 27001 v roce 2007 a jeho obhajoba v roce 2010.

4. 2 Důvod a cíle řešení (včetně doložení jejich měřitelnosti):

Důvod:

Zkvalitnění zásad bezpečnosti informací v činnosti městského úřadu (samostatná i přenesená působnost). Posílení kreditu městského úřadu a důvěra klientů v ochranu svých osobních a citlivých dat.

Cíle:

1. Ochrana osobních a citlivých dat klientů. Ochrana utajovaných informací a zvláštních skutečností.
2. Naplnění ustanovení zákona č. 101/2000 Sb. o ochraně osobních údajů a zákona č. 412/2005 Sb. o ochraně utajovaných informací.
3. Identifikovat rizika v oblasti bezpečnosti informací, analyzovat je a pracovat s nimi. Přijímat adekvátní preventivní opatření k bezpečnosti informací.

4. Týmové řešení bezpečnosti informací u Městského úřadu a posílení odpovědnosti všech zaměstnanců.
5. Zkvalitnění bezpečnosti lidských zdrojů a fyzické bezpečnosti prostředí.
6. Zabezpečení vývoje, údržby a kompatibility informačních systémů a zařízení.
7. Zvládání bezpečnostních incidentů a realizace adekvátních nápravných opatření.
8. Vytyčení hlavních zásad bezpečnosti informací v činnosti úřadu.
9. Stanovení základních postupů a opatření kladených na zaměstnance.
10. Stanovení represivních opatření při porušení zásad bezpečnosti informací.

Měřitelnost:
1. Počet vzniklých nedostatků, neshod a bezpečnostních incidentů.
2. Počet stížností a námětu ke zlepšení ze strany klientů v oblasti bezpečnosti informací.
3. Práce s riziky (minimalizace a eliminace).
4. Pravidelné hodnocení – přezkoumání ISMS vedením.
5. Výsledky vnitřních, certifikačních a dozorových auditů.
6. Benchmarking – srovnání výkonnosti mezi dalšími úřady a odbory.
7. Výsledky kontrol nadřízených.

4.3 Implementace řešení:

- **zainteresované strany**
  vedení města, vedení městského úřadu, zaměstnanci zařazení do městského úřadu, třetí strany smluvně zabezpečující služby, dodávky a činnosti pro městský úřad,

- **odpovědnost za řešení**
  je specifikována ve vnitřním předpisu KODEX ICT a politice bezpečnosti informací pro všechny kategorie zaměstnanců, vedení městského úřadu, fórum bezpečnosti informací a představitele vedení pro ISMS, tajemníka Městského úřadu Žamberk jako hlavního koordinátora činností, který plně podporuje prováděná opatření v rámci zdokonalování kvality činností úřadu,

- **podpora řešení ze strany vedení**
  -tajemník úřadu Žamberk je hlavním koordinátorem činností a plně podporuje prováděná opatření v rámci zdokonalování systému bezpečnosti informací v činnosti úřadu,
  -politika bezpečnosti informací je plně podporována vedením úřadu,
  -pro zabezpečení řízení činností v oblasti bezpečnosti informací a pro implementaci ustanovení daných ČSN ISO/IEC je ustanoveno informační fórum v čele s představitelem vedení pro ISMS,

- **podpora řešení ze strany zaměstnanců**
  politika bezpečnosti informací a zásady ochrany informací byly přijaty všemi zaměstnanci,
  vedoucí zaměstnanci jsou zapojováni do realizace opatření a pravidelně se podílejí na hodnocení a přezkoumávání ISMS,

- **překážky**
  - vzhledem k nutným opatřením se projevilo počáteční nepochopení zásad bezpečnosti informací všemi zaměstnanci,
  - určité finanční, materiální a personální nároky na úřad při zavádění systému,

- **úspěchy**
  - úspěšné zvládnutí certifikačního auditu prováděného společností CQS Praha a udělení certifikátu,
  - zvýšení důvěry v činnost úřadu při přijetí zásad ISMS a zisku certifikátu ISO ze strany klientů a třetích stran,
  - přijetí zásad systému ISMS všemi zaměstnanci,
  - snížení počtu bezpečnostních incidentů a nedostatků v této oblasti na minimum

5. Výsledky řešení

- **Jaké byly hlavní výsledky (uvést pokud možno kvalitativní i kvantitativní ukazatele)?**
  1. Zisk certifikátu ISO 27001, posílení kreditu městského úřadu.
  2. Zvýšení ochrany bezpečnosti informací u úřadu.
  3. Zlepšení ochrany movitého i nemovitého majetku.
  4. Kvalitní plnění ustanovení zák. č. 101/2000 Sb. (o ochraně osobních údajů) a zák. č. 499/2004 S. (o archivnictví a spis. službě).
  5. Posílení povědomí zaměstnanců a zkvalitnění plnění jejich povinností v této oblasti.
  6. Omezení používání a nákladů na přenosné nosiče dat.
  7. Posílení integrity a dostupnosti dat.
  8. Zvýšení kvality zařízení IT.

- **Jaké nástroje pro jejich měření jste použili a jak hodnověrné jsou důkazy?**
  1. Výsledky kontrol nadřízených orgánů.
  2. Výsledky vnitřních a certifikačním auditů.
  3. Benchmarking.
  4. Srovnání vzniklých bezpečnostních incidentů a nedostatků při zahájení realizace opatření a v současnosti.

  Hodnověrné důkazy jsou podloženy jednotlivými zápisy.

- **Vyskytly se nějaké specifické faktory, které mohly ovlivnit úspěch tohoto řešení?**
  1. Počáteční finanční náklady na realizaci předběžných opatření.
  2. Časová náročnost přípravy úřadu k certifikačnímu auditu.
  3. Počáteční kritika opatření a slabá vůle měnit zažité postupy ze strany zaměstnanců úřadu.

  4. **Projevil se nějaký vedlejší negativní či pozitivní účinek?**
  a) Negativní:
  Nárůst pracovních povinností některých zaměstnanců.
  b) Pozitivní:
  Zájem okolních městských úřadů o zavedení zásad bezpečnosti informací – zisk ISO 27001 (osobní návštěvy, konzultace atd.).

6. Inovativnost a přenositelnost dobré praxe[1]

- V čem spočívá inovativnost tohoto řešení? Jak se liší od jiných či podobných aplikací/přístupů?

- Může být/bylo již toto řešení přeneseno/aplikováno v jiné organizaci či sektoru? Pokud ano, které jeho základní prvky? Nebo jste v tomto případě sami využili dobrou praxi od jiných organizací?

- Jaké nejdůležitější poznatky/zkušenosti jste při realizaci řešení získali?

- Jaké je Vaše doporučení pro ty, kteří se zajímají o implementaci tohoto řešení ve své organizaci?

---

[1] *Vyplní pouze uchazeč o cenu MV za inovaci ve veřejné správě*

- Souhlasíte s prezentací Vašeho řešení na nadcházející Národní konferenci kvality ve veřejné správě a v časopise Veřejná správa jakožto s prezentací dobré praxe?

7. Přílohy

Datum: 29.10.2010

Podpis:

Pozn.: V případě ceny udílené za implementaci modelu CAF musí být přílohou závěrečné zprávy sebehodnotící zpráva CAF a na ni navazující akční plán zlepšování. Sebehodnotící zpráva musí obsahovat popis naplnění minimálních kritérií pro udělení daného stupně Ceny MV za model CAF.
Pokud jsou výše uvedené informace součástí sebehodnotící zprávy, lze na ně pouze odkázat.