**

**VZOR**

**důvodová zpráva**

Dokument byl zpracován v rámci realizace projektu

„Efektivní řízení rozvoje obcí jako základní předpoklad efektivnosti výkonu veřejné správy

a poskytování veřejných služeb z úrovně obcí“,

registrační číslo projektu: č.CZ.03.4.74/0.0/0.0/15\_019/0010159

**Důvodová zpráva**

Předkládám Zastupitelstvu/Radě obce/města XXXXXX odsouhlasení návrh znění směrnice č. …/202X Politika bezpečnosti informací Obecního/Městského úřadu XXXXXX (dále také jen úřad).

Tento předkládaný vnitřní organizační předpis je zastřešujícím dokumentem, který bude postupně zahrnovat dílčí systémové, technické a organizační předpisy, sloužící k zajištění kybernetické a informační bezpečnosti úřadu.

Vnitřní organizační předpis je deklarací toho, že vedení úřadu chápe důležitost zajištění kybernetické bezpečnosti informačních systémů úřadu. Na jejich spolehlivém chodu závisí poskytování služeb občanům jakož i plnění legislativních povinností a smluvních závazků. Vedení úřadu tímto deklaruje, že pro řešení kybernetické a informační bezpečnosti zajistí odpovídající finanční, lidské i časové zdroje. Vedení úřadu tímto vnitřním organizačním předpisem deklaruje, že si je vědomo, že při nezavedení odpovídajících opatření v oblasti kybernetické a informační bezpečnosti hrozí minimálně tato rizika

* Riziko reputační – s vysokou jistotou lze předpokládat medializaci případného bezpečnostního incidentu
* Riziko zpochybnění důvěryhodnosti úřadu jako instituce
* Riziko soudních sporů - v případě úniku osobních údajů se dá předpokládat řada soudních sporů se subjekty osobních údajů
* Riziko legislativní neshody, kdy úřad nebude schopen plnit své povinnosti vyplývající z legislativy
* Riziku neplnění smluvních závazků
* Riziko „hledání viníků“ kdy na prvním místě je politická reprezentace
* Riziko finančních ztrát – sankce a pokuty
* a další návazná rizika

Zmíněný vnitřní organizační předpis je deklarací pochopení v něm uvedených principů zajištění kybernetické a informační bezpečnosti. Jeho působnost je v oblasti bezpečnosti informací podstatných pro chod úřadu, a to v jakékoliv podobě, informací v úřadu pořízených, zpracovávaných, ukládaných a i těch získaných vlastní činností i spoluprací s třetími stranami. Z toho je zřejmé, že se dotýká všech zaměstnanců ať už jsou zařazeni do kteréhokoliv organizačního útvaru úřadu.

Vnitřní organizační předpis je závazný pro všechny zaměstnance v jakémkoliv poměru k úřadu stejně tak jako pro smluvní strany.

Tento vnitřní organizační předpis zastřešuje další předpisy, které zavádějí opatření včetně politiky bezpečnosti lidských zdrojů – tzn. zvyšování povědomí (vzdělávání a osvěta) v oblasti kybernetické a informační bezpečnosti, a také zavádějí technická opatření např. ochranu proti škodlivému kódu apod. Tyto navazující předpisy identifikují dílčí oblasti organizačních a technických opatření inspirovaných smyslu zákonem 181/2018 Sb. a navazujícími předpisy a je to zejména:

Politika organizačních a technických opatření která obsahuje tyto dílčí politiky:

1. Politika systému řízení bezpečnosti informací
2. Politika řízení aktiv
3. Politika organizační bezpečnosti
4. Politika řízení dodavatelů
5. Politika bezpečnosti lidských zdrojů
6. Politika řízení provozu a komunikací
7. Politika řízení přístupu
8. Politika bezpečného chování uživatelů
9. Politika zálohování a obnovy a dlouhodobého ukládání
10. Politika bezpečného předávání a výměny informací
11. Politika řízení technických zranitelností
12. Politika bezpečného používání mobilních zařízení
13. Politika akvizice, vývoje a údržby
14. Politika ochrany osobních údajů
15. Politika fyzické bezpečnosti
16. Politika bezpečnosti komunikační sítě
17. Politika ochrany před škodlivým kódem
18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
20. Politika bezpečného používání kryptografické ochrany
21. Politika řízení změn
22. Politika zvládání kybernetických bezpečnostních incidentů
23. Politika řízení kontinuity činností

Na tuto politiku v jednotlivých oblastech navazují příslušné prováděcí směrnice a metodiky.

Účinnost tohoto předpisu bude jednou ročně vyhodnocována a na základě hodnocení bude dokument aktualizován.