**Kybernetická a informační bezpečnost obec XXX**

**Manažerské shrnutí a doporučení**

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

**Preambule**

Základním momentem celé problematiky kybernetické a informační bezpečnosti informační a komunikační infrastruktury obce je to, že za ni zodpovídá statutár. Tento fakt nezávisí na tom, zda obce spadají nebo ne pod zákon 181/2014 Sb. o kybernetické bezpečnosti včetně návazných předpisů.

**Manažerské shrnutí**

Při hodnocení stavu a úrovně zajištění kybernetické a informační bezpečnosti (KIB) v obci XXX bylo zjištěno, že informační a komunikační infrastruktura je co do velikosti opravdu minimální. Jedná se o YY ks PC, které nejsou propojeny do sítě, všechny mají přístup na Internet.. Z tohoto důvodu jsou i opatření kybernetické a informační bezpečnosti minimální na úrovni bezpečnostního řešení od firmy Esset a firewallu, který je součástí operačního systému. Velmi kvalitní je konektivita do Internetu, realizovaná optickým kabelem. Servis výpočetní techniky je zajištěn dodavatelsky firmou XXX Seznam informačních aktiv je veden v rámci evidence majetku.

**Opatření k zajištění kybernetické a informační bezpečnosti obce XXX**

**Bezodkladně přijmout tato opatření:**

1. **Organizační:**
   1. Vyplnit dokument **Katalog aktiv s kontakty**
   2. Zajistit prokazatelné proškolení všech zaměstnanců v základních znalostech toho, jak se chovat a nechovat při používání informačních a komunikačních technologií. Prokazatelnost zajistí tím, že každý zaměstnanec podepíše dokument **Záznam o proškolení\_Kybernetická a informační bezpečnost\_obec XXX**
   3. Zveřejnit a rozšířit mezi všechny zaměstnance dokument **Úvod do problematiky a metodický rámec\_Kybernetická a informační bezpečnost\_obec XXX**, který vysvětluje na příkladech důležitost zajišťování odpovídající úrovně kybernetické a informační bezpečnosti. Seznámení je na bázi dobrovolnosti.

**Průběžně:**

1. ve spolupráci s dodavatelem udržovat aktuální dokument **Katalog aktiv s kontakty.**
2. Ve spolupráci s dodavatelem zajistit vytvoření základní dokumentace pro zajištění kontinuity činností obce XXX v případě výpadku informační a komunikační infrastruktury proto je nutno v **Katalogu a aktiv s kontakty** uvést minimálně:
   1. Priority, podle kterých budou aplikace/systémy restartovány
   2. Popis zálohování – umístění záloh a postup obnovy
   3. Systémy (např.registry) do kterých vedení obce XXX přistupuje vzdáleně
   4. Kontaktní matice – seznam osob, které budou kontaktovány v případě výpadku s vyznačením, kdo bude informován a kdo se na řešení bude aktivně podílet. Do kontaktní matice uvést všechny relevantní kontakty

**Závěr**

Je velmi důležité uvědomit si, že zajišťování kybernetické a informační bezpečnosti je nikdy nekončící proces, který musí reagovat na stále se zhoršující bezpečnostní situaci v kybeprostoru a na bezpečnostní trendy. Klíčovými v této oblasti nejsou ani tak technologie, i když samozřejmě jsou důležité a jejich správné nastavení minimalizuje prostor pro to, aby uživatel udělal chybu. Klíčovou je obezřetnost uživatelů a té nelze dosáhnout jinak než neustálou osvětou a nekompromisním vyžadováním zodpovědného chování ve vztahu ke kybernetické a informační bezpečnosti.