**

**VZOR**

**záznam o bezpečnostním školení zaměstnance v oblasti bezpečnosti informací**

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

### Z Á Z N A M

### o bezpečnostním školení zaměstnance v oblasti bezpečnosti informací

Školení provedl(a) ……..……………………………………….......................................................

Funkce ………………………………………………………………………........................

**Základní povinnosti**

Každý zaměstnanec je odpovědný za nakládání s informacemi a využití prostředků jemu svěřených. Získané informace smějí být využívány výhradně k plnění pracovních úkolů a jakékoliv jiné využití (například jejich neoprávněné kopírování nebo poskytování mimo úřad) se považuje za hrubé porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané činnosti.

Pro zajištění bezpečnosti informací jsou zaměstnanci povinni k řádnému výkonu své služební funkce dodržovat zejména tyto zásady:

1. Používejte služební zařízení (zejména PC a Notebook) pouze k plnění svých služebních nebo pracovních povinností, v souladu s účelem, ke kterému je zařízení určeno
2. Neprovádějte jakékoliv neoprávněné zásahy do operačního systému nebo software (např. instalaci vlastního SW, změna konfigurace)
3. U informací rozlišujte osoby nebo skupiny osob, komu jsou určeny nebo mohou být poskytovány s ohledem na jejich citlivost.
4. Pečlivě si chraňte svá zařízení před odcizením či zneužitím a přístupové údaje před jejich odhalením a zneužitím. Nepoužívejte služební emailovou adresu ani služební heslo pro externí webové služby. Přístupové údaje (zejména heslo nebo PIN) si nikam nepoznamenávejte (např. na papír, do diáře či telefonu). Nevyužívejte stejné přístupové údaje k více účtům, aplikacím či zařízením. Je nutné používat bezpečná hesla a pravidelně je měnit. Dodržujte zásadu, že hesla a PINy se nikomu nesdělují.
5. Neotvírejte neznámé emaily a zejména jejich přílohy, neotevírejte neznámé, neočekávané soubory. Soubory, které mají příponu typu exe, com, scr, pif a další mohou vést k ohrožení informačních systémů. Pokud se ve složce, kam se stahují soubory z Internetu (webu), objeví neznámý soubor, neotevírejte ho. Může jít o infikovaný soubor, který byl bez vašeho vědomí stažen z nedůvěryhodné stránky. Oznamte tuto skutečnost určenému pracovníkovi nebo přímému nadřízenému.
6. Nenastavujte ani nepožadujte nastavení automatického přesměrování služebních e-mailů do soukromých e-mailových schránek. Je to jedna z nejnebezpečnějších aktivit, která může vést k úniku informací.
7. Dodržujte zásadu uzamčené obrazovky stisknutím kláves Win+L či využití zkratky Ctrl+Alt+Del) a prázdného stolu (neponechávejte dokumenty bez dozoru volně na stole). Zamykejte zařízení (např. PC a notebook) pokud s ním nepracujete, a to zejména při odchodu z kanceláře.
8. Dbejte na zásady bezpečnosti při fyzickém přístupu do kanceláří a vyhrazených prostor. Neponechávejte v kanceláři jiné osoby bez dozoru a při odchodu kancelář vždy zamykejte. Dbejte na to, aby do vyhrazených prostor nevstupovaly neoprávněné osoby.
9. Používejte přidělená výměnná média (např. flash disk, CD, DVD) vždy zodpovědně a bezpečně. Nenechávejte je bez dozoru, a pokud je to možné tak je šifrujte. V případě nalezení neznámého výměnného média jej nepřipojujte ke svému zařízení bez předchozího prověření antivirem. Oznamte tuto skutečnost určenému pracovníkovi nebo přímému nadřízenému.
10. Nesdílejte služební informace (dokumenty) cestou veřejných úložišť (Dropbox, Úschovna, Úložna apod.).
11. Nenavštěvujte nedůvěryhodné webové stránky a neklikejte na odkazy na neznámé či podezřelé webové stránky. Mezi typické znaky nedůvěryhodné webové stránky patří velké množství reklamy, vyskakovací okna, stránky měnící se bez akce uživatele, zahájení stahování bez vědomí uživatele apod. Preferujte webové stránky, které důvěrně znáte a jsou zabezpečeny protokolem https, to znamená, že adresa příslušné stránky začíná takto https:// na začátku adresy.
12. V případě zjištění nestandardního chování aplikace, bezpečnostní události (zejména neoprávněného přístupu) nebo výskytu neznámých a nesrozumitelných jevů, nepodléhejte panice, ponechte vše, jak je, počítač nevypínejte a nahlaste tuto skutečnost určenému pracovníkovi nebo přímému nadřízenému.
13. Neotevírejte neznámé soubory. Pokud se ve složce, kam se stahují soubory z Internetu (webu), objeví neznámý soubor, neotevírejte ho. Může jít o infikovaný soubor, který byl bez vašeho vědomí stažen z nedůvěryhodné stránky. Oznamte tuto skutečnost určenému pracovníkovi nebo přímému nadřízenému.
14. Nepožadujte po příslušných odbornících, aby vám zajistili výjimky z uvedených opatření. Jedna „vynucená“ výjimka může být právě tou útočníkem zneužitou „dírou“ do systému.

**Hlášení bezpečnostních událostí a incidentů**

Bezpečnostní incident je událost, při které dochází k selhání nebo úmyslnému či neúmyslnému ohrožení bezpečnosti informací. Zaměstnanec je povinen nahlásit neprodleně zjištěný incident, nebo podezření, že incident nastal určenému pracovníkovi.

**Porušení zásad bezpečnosti informací**

Porušení zásad, postupů a pravidel bezpečnosti informací je posuzováno jako porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci.

Zaměstnanec potvrzuje svým podpisem, že byl(a) seznámen(a) se zásadami bezpečnosti informací

Titul, jméno a příjmení zaměstnance………………………....................................................................

V ……………. dne ……………. ………………………...........................

 podpis zaměstnance