Příloha č. 3

MĚSTSKÝ ÚŘAD NOVÝ BOR

Pracoviště informačních technologií

nám. Míru 1, 473 01 Nový Bor, tel. 487 712 311, fax 487 726 160, e-mail: epodatelna@novy-bor.cz

Bezpečnostní pravidla v oblasti Informačních a komunikačních technologií (ICT) pro práci v informačním systému (IS) Města Nový Bor (MUNB)

Externí subjekt je při práci v IS MUNB povinen dodržovat v oblasti ICT tato bezpečnostní pravidla:

1. **Přístup do IS MUNB**
   - 1.1. Přístup jiných subjektů k ICT MUNB (dále jen „druhá smluvní strana“) je možný pouze na základě smluvně ošetřeného vztahu s městem Nový Bor.
   - 1.2. Druhá smluvní strana je povinna dodržovat bezpečnostní pravidla ICT pro práci v IS MUNB a nese v souladu s platnou legislativou a předpisy svůj díl odpovědnosti za nedodržení či porušení pravidel, případně za škody vzniklé v důsledku bezpečnostních incidentů, které zavinila.
   - 1.3. Všechny povolené způsoby přístupu, povolené časy pro přístup, přístupové údaje a přidělená oprávnění musí být písemně dohodnuty mezi smluvními stranami. Tyto údaje jsou důvěrné a jsou platné jen po dobu platnosti smlouvy.
   - 1.4. Druhá smluvní strana je odpovědná za používání jim přiděleného přístupu do IS MUNB, za svou činnost v IS MUNB a při práci s informacemi.
   - 1.5. Přistupovat k ICT MUNB mohou pouze poučení pracovníci druhé smluvní strany. Druhá smluvní strana zajistí před zahájením prací poučení a proškolení všech svých pracovníků a subdodavatelů, kteří budou přistupovat k ICT MUNB.
   - 1.6. Přístup a přístupová oprávnění jsou přidělena pouze v rozsahu nezbytně nutném pro výkon smluvních závazků.
   - 1.7. Pracovníci druhé smluvní strany jsou povinni řídit se pokyny oprávněných osob a dalších pracovníků pracoviště IT MUNB.
   - 1.8. Činnost druhé smluvní strany v IS MUNB může být monitorována. Pověření pracovníci MUNB mohou evidovat přístupy a ověřovat dodržování stanovených bezpečnostních pravidel.
2. **Vzdálený přístup**
   - 2.1. Vzdálený přístup do IS MUNB je možný pouze dohodnutým způsobem z pracovní stanice, která má aktivní a aktuální antivirovou ochranu a nainstalovány všechny bezpečnostní záplaty operačního systému vydané výrobcem.
   - 2.2. Pro zvýšení bezpečnosti je vzdálený přístup povolen pouze z konkrétních IP adres druhé smluvní strany.
   - 2.3. Přihlašovací heslo sdělují oprávněné osoby Objednatele oprávněným osobám Zhotovitele. Přihlašovací účet je mimo dobu používání neaktivní. Aktivace účtu provádí oprávněné osoby Objednatele před použitím vzdáleného přístupu na základě žádosti oprávněné osoby Zhotovitele.
3. **Fyzický přístup k ICT**
   - 3.1. Fyzický přístup k prostředkům ICT je možný pouze na základě smluvního vztahu (servisní a dodavatelské organizace, dohody o provedení práce apod.) nebo se souhlasem určené odpovědné osoby, kterou může být vedoucí pracoviště IT nebo vlastník (manažer) aktiva MUNB.
   - 3.2. Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze za stálé přítomnosti a dozoru odpovědných pracovníků pracoviště IT a se souhlasem vedoucího pracoviště IT.
   - 3.3. Při opuštění pracoviště je vždy nutné provést vhodným způsobem jeho zajištění dle pokynů vedoucího pracoviště IT MUNB.
4. **Ochrana dat a informačních aktiv**
   - 4.1. Druhá smluvní strana odpovídá za všechna převzatá data (elektronická a tištěná), způsob jejich použití a ochranu před neoprávněným přístupem a zneužitím.
   - 4.2. Není-li ve smlouvě stanoveno jinak, před ukončením smluvního vztahu druhá smluvní strana vrátí všechna převzatá data.
   - 4.3. Druhá smluvní strana je do protokolárního předání pracovníkům MUNB odpovědná za všechna zpracovávaná aktiva a je povinna je odpovídajícím způsobem zabezpečit.
   - 4.4. Pracovní data se ukládají pouze na místa, určená pověřenou osobou MUNB.

4.5. Pokud druhá smluvní strana při práci v IS MUNB přijde do styku s osobními údaji dle zákona č. 101/2000 Sb. nebo jinými neveřejnými informacemi, je povinna o zjištěných skutečnostech zachovávat mlčenlivost a zajistit jejich utajení.

4.6. Nepotřebná data (elektronická, na mediích i papírová) musí být vždy neprodleně zlikvidována.

4.7. Druhá smluvní strana je povinna dodržovat zásady ochrany proti virům a škodlivým kódům.

4.8. Všechny zásahy na serverech musí být předem odsouhlaseny vedoucím pracoviště IT a zaznamenány stanoveným způsobem MUNB.

5. Bezpečnostní incidenty

5.1.1. Druhá smluvní strana je povinna neprodleně hlásit manažerovi ISMS MUNB porušení těchto pravidel, všechny zjištěné neobvyklé události, které jsou, nebo mohou být bezpečnostními incidenty a zranitelná místa, a účinně pomáhat při jejich prošetřování a odstraňování.

5.1.2. Druhá smluvní strana je povinna hlásit všechny zjištěné bezpečnostní nedostatky nebo nesoulad se skutečností.

5.1.3. Druhé smluvní straně není povoleno řešení bezpečnostních incidentů a odstraňování nedostatků či nesouladů vlastními silami bez předchozího schválení manažerem ISMS MUNB.

6. Používání internetu

6.1. Druhá smluvní strana může používat při práci v IS MUNB internet pouze pro pracovní účely při dodržování všech obecně závazných právních předpisů České republiky a jednat v souladu s dobrými mravy a všeobecně uznávanými morálními a etickými normami. Uživatel zejména nesmí porušovat zákonem chráněná práva poskytovatele a třetích osob. Uživatel nesmí využívat službu k obtěžování třetích osob, zejména rozesíláním nevyžádaných dat. Uživatel se zavazuje, že bude využívat službu pouze v rámci platných právních předpisu a že bude respektovat etická pravidla užívání sítě Internet. Stahování souborů, používání FTP a jiných služeb je možné jen po dohodě se správcem systému MUNB.

6.2. Pokud není ve smlouvě stanoveno jinak, není povoleno využívat elektronickou korespondenci z prostředí MUNB.

7. Tisk

7.1. Pokud bude druhé smluvní straně umožněn tisk na tiskárnách města, je povinna šetřit spotřební materiál a tištěné dokumenty zabezpečit proti neoprávněnému přístupu jak během tisku, tak i po jeho vytisknutí až do jejich bezpečné likvidace.

8. Účty a hesla

8.1. Druhá smluvní strana smí používat pouze jí přidělené přihlašovací účty. Tyto účty jsou chráněny heslem.

8.2. Heslo musí splňovat aktuální požadavky na kvalitu a platnost a musí být uchováno v tajnosti.

8.3. Názvy přihlašovacích účtu a hesla nesmějí být sděleny žádné neoprávněné osobě.

8.4. V případě porušení bezpečnostních pravidel mohou být druhé straně přístupové účty zablokovány nebo zcela odebrány.

Druhé smluvní straně je přísně zakázáno vykonávat jiné než dohodnuté činnosti, přistupovat k jiným než povoleným prostředkům, serverům a datům nebo provádět jakékoli úkony směřující k zjišťování rozsahu přidělených oprávnění, dostupnosti