

Bezpečnostní pravidla pro práci v informačním systému (IS) Města Kroměříže (MK)

ICT (informační a komunikační technologie) jsou veškeré informační technologie používané pro komunikaci a práci s informacemi

IS (Informační systém) je celek složený z počítačového hardwaru, souvisejícího softwaru a dat.

Správce IS je pracovník Odboru informačních technologií Městského úřadu Kroměříž (MěÚ KM). Je uveden jako odpovědná osoba předávajícího v předávacím protokolu o předání přihlašovacích údajů.

Odpovědná osoba je seznam osob uvedených ve smlouvě, s právem jednat v technických nebo smluvních věcech.

Druhá smluvní strana je subjekt, kterému je umožněn přístup k IS MK a dále všichni jeho pracovníci, poddodavatelé apod.

Při porušení bezpečnostních pravidel druhou smluvní stranou mohou být přidělené přístupové účty zablokovány nebo zcela odebrány.

1. Přístup k IS MK

- a) Přístup jiných subjektů (druhé smluvní strany) k IS MK je možný pouze na základě smluvně ošetřeného vztahu s MK.
- b) Druhá smluvní strana je povinna používat pouze jí přidělené přístupy a povolené způsoby přístupu, (fyzické přístupy, přístupové údaje, povolené časy pro přístup a přidělená oprávnění), a je odpovědná za jejich používání. Přidělené údaje jsou pro druhou stranu závazné, jsou důvěrné a jsou platné jen po dobu platnosti smlouvy. Tyto údaje jsou uvedeny ve smlouvě nebo v Předávacím protokolu k účtu.
- c) Přístupy a přístupová oprávnění jsou přidělena pouze v rozsahu nezbytně nutném pro výkon smluvních závazků. Druhá smluvní strana nesmí bez souhlasu Správce IS vytvářet nové přístupové účty a do přidělených účtů a oprávnění zasahovat a měnit je. Pokud druhá smluvní strana zjistí, že skutečná oprávnění jsou odlišná od dohodnutých, neprodleně na to upozorní odpovědné osoby nebo Správce IS.
- d) Přístupovat k IS MK mohou pouze poučení pracovníci druhé smluvní strany. Druhá smluvní strana zajistí před zahájením prací poučení a proškolení všech svých pracovníků a subdodavatelů, kteří budou přístupovat k IS MK.

2. Práce v IS MK

- a) Druhá smluvní strana je povinna dodržovat bezpečnostní pravidla a stanovené postupy pro práci v IS MK 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.
- b) Je přísně zakázáno vykonávat jiné než dohodnuté činnosti, přistupovat k jiným než povoleným prostředkům, serverům a datům. Dále je zakázáno provádět jakékoli úkony směřující k zjišťování rozsahu přidělených oprávnění, dostupnosti síťových prostředků a služeb a způsobů zabezpečení a provádět pokusy o jejich překonání.
- c) Druhá smluvní strana nesmí vytvářet žádné přístupové cesty do IS MK a měnit přístupová oprávnění. Tyto změny může provádět Správce IS na základě písemné žádosti.
- d) Činnost druhé smluvní strany v IS MK je monitorována a evidována. Pověření pracovníci MK mohou ověřovat dodržování stanovených bezpečnostních pravidel a zakázat neoprávněné aktivity.
- e) Pracovníci druhé smluvní strany jsou povinni řídit se pokyny Odpovědné osoby (uvedených ve smlouvě), Správce IS a dalších pracovníků Odboru informačních technologií.

- f) Druhá smluvní strana je povinna předávat Správci IS informace o provedených zásazích a změnách, a bez zbytečného prodlení je promítnout do dokumentace. Všechny změny, které mohou ovlivnit bezpečnost IS MK, musí být předem projednány a schváleny Správcem IS.

3. Účty a hesla

- a) Druhá smluvní strana je povinna chránit přístupové účty heslem. Druhá strana nesmí sdělit názvy účtů a hesla žádné neoprávněné osobě. Heslo musí splňovat aktuální požadavky MK na kvalitu a platnost a musí být uchováno v tajnosti. Hesla musí být vždy předávána bezpečným způsobem. Pokud je to možné, musí být použita více faktorová autentizace.
- b) Standardně jsou přístupové účty neaktivní. V případě potřeby mohou jejich aktivaci schválit a zajistit odpovědné osoby. Žádost musí obsahovat informace o prováděných činnostech a předpokládané době prací. Druhá smluvní strana nesmí bez předchozího upozornění provádět jiné než nahlášené práce.

4. Vzdálený přístup a vzdálená údržba

- a) Vzdálený přístup do IS MK je možný pouze dohodnutým způsobem. Vzdálený přístup musí být vždy šifrován.
- b) Druhá smluvní strana smí vzdáleně přistupovat do IS MK pouze z pracovní stanice, která má nainstalovaný podporovaný operační systém, nainstalovány všechny bezpečnostní záplaty operačního systému vydané výrobcem, a má aktivní a aktuální antivirovou ochranu.
- c) Druhá smluvní strana smí vzdáleně přistupovat do IS MK pouze z ověřených konkrétních IP adres předem odsouhlasených Správcem IS.
- d) Pracovní stanice určené k přístupu do IS MK ze vzdálené lokality musí být druhou smluvní stranou fyzicky zabezpečeny proti přístupu neoprávněných osob.

5. Zabezpečení fyzického přístupu k IS

- a) Servery, síťové komponenty a další ICT zařízení jsou zabezpečeny proti fyzickému přístupu. Přístup do místností se servery s citlivými daty a přístup k síťovým zařízením je regulován a odpovídajícím způsobem monitorován. Pokud fyzické zabezpečení citlivých dat není dostatečné, musí být zabezpečena šifrováním.
- b) Opravy ICT komponent mohou být prováděny pouze na základě smluvně ošetřeného vztahu s MK.
- c) Fyzický přístup k prostředkům IS je umožněn pouze druhým smluvním stranám (servisní a dodavatelské organizace, dohody o provedení práce apod.), u kterých udělení přístupu vyplývá z uzavřené smlouvy. Fyzický přístup k prostředkům IS je možné uskutečnit pouze se souhlasem Správce IS nebo vedoucího Odboru informačních technologií.
- d) Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků Odboru informačních technologií nebo jimi pověřených osob.
- e) Pro přímé připojení (v prostorách MK) do IS MK smí být použita pouze přidělená technika MK. Připojování cizí techniky do vnitřní sítě MK je zakázáno. Výjimky povoluje Správce IS.
- f) Na přidělenou techniku MK nesmí být bez souhlasu pověřené osoby nahráván, instalován nebo z ní odebírán žádný software, dále bez souhlasu pověřené osoby nesmí být upravována konfigurace přidělené techniky.
- g) Při opuštění pracoviště musí druhá smluvní strana provést jeho zajištění (pracovní stanice, nosiče dat, papírové dokumenty) před neoprávněným přístupem.
- h) Druhá smluvní strana je povinna uchovávat přenosná paměťová média na bezpečném místě, např. v uzamčené skříni, stole nebo místnosti. Originální datová média a záložní kopie citlivých souborů musí být chráněna nejen proti odcizení a zneužití, ale i proti poškození nebo zničení.
- i) Druhá smluvní strana je povinna chránit přidělené pracovní stanice a data na nich uložená proti odcizení, proti neoprávněnému přístupu a proti poškození nebo zničení.

6. Ochrana dat a informačních aktiv

- a) Druhá smluvní strana je povinna chránit všechna data MK, se kterými přijde do styku. Všechny nové aplikace a aktualizace musí být ověřeny v testovací prostředí. Používat ostrá data pro zkušební a testovací účely je zakázáno. Výjimku může v odůvodněných případech povolit pouze vedoucí Odboru informačních technologií.
- b) Druhá smluvní strana odpovídá za všechna převzatá data (elektronická a tištěná), způsob jejich použití a ochranu před neoprávněným přístupem a zneužitím. Není-li ve smlouvě stanoveno jinak, před ukončením smluvního vztahu druhá smluvní strana vrátí všechna převzatá data a všechny jejich kopie bezpečně zlikviduje.
- c) Druhá smluvní strana je do protokolárního předání pracovníkům MK odpovědná za všechna zpracovávaná aktiva a je povinna je odpovídajícím způsobem zabezpečit.
- d) Ukládání pracovních dat je možné pouze na místa, která určí odpovědná osoba.
- e) Druhá smluvní strana nesmí zobrazovat, měnit, mazat nebo kopírovat citlivá data, zejména pak osobní údaje, pokud to nesouvisí se schváleným účelem přístupu.
- f) Vadná zařízení (včetně pevných disků) s nešifrovanými citlivými daty mohou být druhou smluvní stranou předány externím servisním specialistům pouze po schválení Správcem IS nebo vedoucím Odboru informačních a komunikačních technologií.
- g) Pokud druhá smluvní strana při práci v IS MK přijde do styku s osobními údaji dle platné legislativy nebo jinými neveřejnými informacemi, je povinna o zjištěných skutečnostech zachovávat mlčenlivost a zajistit jejich utajení.
- h) Nepotřebná data (elektronická, na mediích i papírová) musí být druhou smluvní stranou vždy neprodleně skartována.
- i) Druhá smluvní strana je povinna všechny zásahy na serverech předem odsouhlasit se Správcem IS a zaznamenat stanoveným způsobem.

7. Ochrana proti škodlivým kódům

- a) Druhá smluvní strana je povinna všechny servery a pracovní stanice v IS MK a pracovní stanice druhé smluvní strany, které se připojují k IS MK, vybavit antivirovým skenerem. Výjimky schvaluje Správce IS.
- b) Pokud některé aplikace nabízejí možnost zvýšené ochrany, musí být odpovídajícím způsobem nastavena. Způsob nastavení schvaluje Správce IS.
- c) Nebezpečné typy souborů jsou blokovány na hranicích bezpečnostního perimetru. Výjimky schvaluje v řádně odůvodněných a zdokumentovaných případech Správce IS.
- d) Druhá smluvní strana je povinna dodržovat zásady ochrany proti virům a škodlivým kódům nejen pro nastavení a využívání prostředků MK, ale i na přístupových bodech a svých vlastních zařízeních.

8. Bezpečnostní incidenty

- a) Druhá smluvní strana je povinna neprodleně hlásit odpovědným osobám porušení těchto Bezpečnostních pravidel, všechny zjištěné neobvyklé události, které jsou, nebo mohou být bezpečnostními incidenty, zjištěná zranitelná místa, nedostatky a nesoulady. Při jejich prošetřování a odstraňování je povinna poskytnout účinnou součinnost.
- b) Druhé smluvní straně není povoleno řešení bezpečnostních incidentů a odstraňování nedostatků či nesouladů vlastními silami bez předchozího schválení Správcem IS.

9. Používání internetu

- a) Druhá smluvní strana může používat při práci v IS MK internet pouze pro účely plnění smlouvy a za podmínky dodržování všech všeobecně uznávaných bezpečnostních pravidel, platných pro práci s internetem. Stahování souborů, používání FTP a jiných služeb je možné jen po dohodě se Správcem IS.
- b) Pokud není ve smlouvě stanoveno jinak, není povoleno využívat elektronickou korespondenci z prostředí MK.

10. Tisk

- a) Druhá smluvní strana může tisknout na tiskárnách MK pouze s povolením odpovědné osoby. Tisknout je povoleno pouze dokumenty související s předmětem smlouvy a při tisku je nutno šetřit spotřební materiál.
- b) Druhá smluvní strana je povinna zabezpečit tištěné dokumenty proti neoprávněnému přístupu jak během tisku, tak i po jeho vytisknutí, až do jejich bezpečné skartace.

11. Použití kryptografických technik

- a) Kryptografické metody musí být druhou smluvní stranou použity vždy, jestliže není možné bezpečnost dat nebo komunikace zaručit jinými způsoby. Jedná se např. o přenosy citlivých dat prostřednictvím nedůvěryhodných sítí nebo přístup externích subjektů k citlivým zdrojům.
- b) Druhá smluvní strana je oprávněna použít pouze takové kryptografické algoritmy a protokoly a v takovém užití (např. odpovídající délky klíčů), které jsou podle platných standardů všeobecně považovány za bezpečné.
- c) Druhá smluvní strana není oprávněna použít proprietární nebo obecně neuznávané algoritmy, výjimky povoluje Správce IS.