****

Sp.zn. OT/3680/2023

Č.j. MUHU/26497/2023/Sa

Bezpečnostní směrnice

směrnice č. SM/6/2023/RM

|  |  |
| --- | --- |
| Organizace:(dále „Organizace“) | Město Humpolec, Horní náměstí 300, 396 22 Humpolec IČO 00248266 |
| Vypracoval: | Ing. Milan SeidlerMgr. Jiří Fiala, tajemník MěÚ |
| Schválil: | Rada města Humpolce, usnesením č. xx/18/RM/2023 | Dne 13/9 2023 |
| Kontrolou provádění směrnice je pověřen: | Mgr. Jiří Fiala, tajemník MěÚ |
| Datum platnosti od: | 14/9 2023 |
| Datum účinnosti od: | 1/10 2023 |
| Tato směrnice ruší interní směrnici č. 1/2008, kterou se stanoví pravidla pro ochranu majetku města v objektech Městského úřadu Humpolec ze dne 1. ledna 2008 a Bezpečnostní směrnici č.1/2018 ze dne 6. června 2018.Tato směrnice upravuje bezpečnostní pravidla v oblasti IT a zabezpečení prostor užívaných Městským úřadem Humpolec (dále jen „MěÚ“) včetně pravidel pro ochranu majetku města v následujících objektech MěÚ: č.p. 300 a 301 na Horním náměstí, č.p. 253 na Dolním náměstí a č.p. 1525 v ul. Příčná (dále jen „budova MěÚ“). |

Část I.

Zkratky, pojmy a lokalizace umístění souvisejících dokumentů

|  |  |
| --- | --- |
| Pojem/ zkratka | Význam |
| Citlivý OÚ | Dle čl. 9 GDPR se jedná o:* Údaje o rasovém a etnickém původu
* Údaje o politických názorech
* Údaje ukazující na náboženské vyznání nebo filosofické přesvědčení
* Údaje o odborové příslušnosti
* Genetické údaje
* Biometrické údaje umožňující identifikaci jednotlivce
* Údaje o zdravotním stavu
* Údaje o sexuálním životě a sexuální orientaci
* Údaje o odsouzení v trestných věcech
 |
| Dostupnost | Jaký může mít následek, když nebude OÚ po daný čas dostupný |
| DPO | Zkratka pro pověřence (viz Pověřenec) v rámci GDPR |
| Důvěrnost | jaký může mít následek ztráta daného OÚ |
| GDPR | Nařízení EU 2016/679 ze dne 27.4.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů |
| ICT | Informační a komunikační technika |
| Integrita | Co bude mít za následek neoprávněná změna OÚ |
| IS | Informační systém – program, nebo soubor programů určených pro zpracování dat včetně OÚ |
| OS | Operační systém |
| OÚ | Jakýkoliv údaj nebo kombinace údajů, pomocí kterých je možno osobu/subjekt jednoznačně identifikovat (např. PČR) |
| PC, počítač | Pracovní stanice uživatele |
| PČR | Policie České republiky |
| Pověřenec | Osoba povinná pro některé typy organizací, která plní úkoly v rozsahu specifikovaném v čl. 37 GDPR a zajišťuje:* monitorování souladu s GDPR
* řízení činnosti interní ochrany dat
* školení zaměstnanců ve zpracování dat OÚ
* provádění interních auditů
* spolupracuje s ÚOOÚ
	+ musí oznámit porušení ochrany dat (do 72 hodin od narušení bezpečnosti na ÚOOÚ)
	+ působí jako kontaktní místo pro ÚOOÚ v záležitostech týkajících se zpracování vč. předchozí konzultace příp. vedení konzultací v jakékoliv jiné věci
* působí jako kontaktní místo pro subjekty zpracovávaných OÚ
 |
| Pseudonymizace | Náhrada osobního údaje nějakým identifikátorem, na základě kterého, již nelze SÚ identifikovat |
| Správce | Právnická nebo fyzická osoba, která určuje účely a prostředky zpracování osobních údajů, odpovídá za ochranu OÚ, určuje účel a prostředky zpracování OÚ, odpovídá za ochranu OÚ (musí zajistit důvěrnost, integritu a dostupnost OÚ odpovídajícími prostředky). Musí být schopna prokázat, co je v jeho případě „odpovídající“ prostředek na základě analýzy rizik. V rámci tohoto dokumentu také „Organizace“ |
| SÚ | Subjekt údaje (ke kterému se váže daný OÚ) – osoba (v případě dítěte za něj jedná jeho zákonný zástupce), nebo firma, příp. jiná instituce |
| ÚOOÚ | Úřad na ochranu osobních údajů |
| WP29 | Skupina v rámci EU řešící výklad GDPR |
| Zpracovatel | Obecně subjekt, kterého pověřil Správce zpracováváním OÚ (např. na základě smlouvy – externí účetní, provozovatel cloudu, kde organizace ukládá data (je možno aby správce přenesl odpovědnost na provozovatele cloudového řešení a příp. udělal i přísnější podmínky)Má stejnou odpovědnost jako správce (např. musí být schopen prokázat, co je v jeho případě „odpovídající“ prostředek na základě analýzy rizik.)Povinná smlouva mezi správcem a zpracovatelem (pro všechny případy, kdy dodavatelská firma provozuje službu, při níž dochází ke zpracování OÚ – mzdy, outsourcing, IS, …) |

Část II.

Úvodní ustanovení

Tato směrnice upravuje pravidla pro ochranu majetku a osobních dat zaměstnanců organizace, osob, které jsou k organizaci v jiném pracovně právním vztahu (dohoda o provedení práce, dohoda o pracovní činnosti) nebo jiný právní vztah (smlouva o dílo, nájemní smlouva, příkazní smlouva apod.), a dalších osob, které poskytují své osobní údaje organizaci k využití (dále také jen „zaměstnanec“).

Cíle směrnice:

* Stanovení pravidel pro ochranu majetku
* Stanovení bezpečnostních pravidel pro práci s osobními údaji pro doložení plnění základních principů GDPR (odpovědnost, mimo jiné pro zajištění důvěrnosti, dostupnosti a integrity).

Část III. Obecné podmínky zabezpečení

Každý zaměstnanec zařazený do Městského úřadu Humpolec je povinen chránit majetek města před poškozením, ničením a zneužitím. Je povinen si počínat tak, aby nedocházelo ke škodám na zdraví osob, ke škodám na majetku, ani k neoprávněnému majetkovému prospěchu.

1. **Fyzická bezpečnost**

Předměty, materiál a jiné věci se mohou z objektu organizace vynášet pouze s vědomím nadřízeného zaměstnance.

Budova organizace jako celek, jednotlivé místnosti ani prostředky ICT pracovišť nejsou volně přístupné veřejnosti. V časově omezené době je přístup do vyjmenovaných částí budovy a oploceného areálu okolo budovy za specifikovaných podmínek přístupný veřejnosti, nebo specifikované skupině osob.

Dokumenty, zejména s osobními údaji nebo pro organizaci citlivými údaji, nejsou volně přístupné veřejnosti a jsou zabezpečeny minimálně v uzamykatelné kanceláři, která je při odchodu zaměstnanců organizace z této kanceláře posledním odcházejícím zaměstnancem uzamčena. Dokumenty s citlivými osobními údaji jsou navíc v rámci kanceláře uloženy v uzamykatelných skříních/šuplících, které jsou uzamčeny při odchodu zaměstnance, který odpovídá za zpracovávání těchto údajů.

Po uzamčení budovy/místnosti/skříně/šuplíků zaměstnanec uloží klíč na bezpečné místo (dle směrnice nebo dle písemných pokynů nadřízeného), nebo si klíče odnese s sebou. Zaměstnanec organizace odpovídá za zabezpečení jemu svěřených klíčů organizace.

V případě jednání s klientem zaměstnanec zabezpečí, aby klient nemohl vizuálně nebo sluchem získat osobní údaje třetích stran, nebo aby klientem předávané osobní údaje nebyly třetími stranami sluchem nebo vizuálně zjistitelné. Zvláštní pozornost je nutno věnovat zejména při předávání citlivých osobních údajů.

1. **Personální bezpečnost**

Přístup do prostředků ICT a provozovaných IS mohou mít pouze zaměstnanci organizace, kteří jsou k tomu zmocněni z výkonu své funkce, nebo dle pokynů tajemníka.

Správu prostředků ICT, příp. IS zajišťuje osoba pověřená tajemníkem.

Rozsah přístupových oprávnění musí odpovídat zastávané funkci. O přidělení a odebrání přístupových práv rozhoduje tajemník, nebo jím pověřená osoba (správce ICT, příp. správce daného IS).

Omezení přístupových práv uživatelů na úrovni operačního systému:

* je zakázána instalace aplikací, stahování filmů, streamování, apod.
* je zakázána instalace ovladačů (mimo jiné omezení možnosti využití vlastních flash disků).

Rozsah oprávnění externího uživatele určuje tajemník.

1. **Režimová bezpečnost**

Přístup do budovy organizace je chráněn minimálně bezpečnostními dveřmi s bezpečnostním zámkem a mimo provozní dobu elektronickým zabezpečovacím systémem (EZS).

Přístup k prostředkům ICT mohou mít pouze oprávnění uživatelé a správci. Toto je zajištěno autentizací uživatelů minimálně heslem, nebo obdobnou technologií zabezpečení. Po autentizaci uživatele není dovoleno nechat prostředek ICT bez dozoru v nezabezpečené místnosti. Po autentizaci osoby s právy administrátora není dovoleno ponechat prostředek ICT nezabezpečený.

Nástroje určené pro zabezpečení (heslo, čip, klíče, PIN) není povoleno poskytnout jiné osobě nebo je umístit tak, že jsou zneužitelné jinou osobou (nezapisovat si heslo na klávesnici nebo monitor, nechávat klíče od skříní na nezabezpečeném místě v kanceláři).

Cizím osobám je vstup do objektu mimo pracovní dobu povolen pouze s vědomím tajemníka úřadu nebo starosty města.

Pobyt na pracovišti ve dnech pracovního volna nebo pracovního klidu povoluje tajemník úřadu nebo starosta města.

Osoby, vykonávající úklidové, opravářské a jiné práce na objektech se musí zdržovat pouze tam, kde konkrétní práci vykonávají. Odpovědnost má a dozor vykonává pověřená osoba.

V souladu s vnitřním předpisem MěÚ je v rámci jednotlivých odborů úřadu pověřen zaměstnanec odpovídající za provoz elektrického spotřebiče. Pověřená osoba byla řádně poučena o bezpečnosti a ochraně zdraví při manipulaci s elektrickým přístrojem (seznam pověřených osob je uložen ve složce školení BOZP). Při odchodu z budovy odpovídají pověření zaměstnanci za vypnutí spotřebiče ze zásuvky el. sítě.

1. **Programová bezpečnost**

Programové vybavení se skládá pouze ze systémového a aplikačního SW udržovaného v aktuálních verzích: z operačního systému WINDOWS (s ovladači pro HW a aplikačního SW, který je standardní součástí tohoto OS), Adobe Readeru, internetového prohlížeče, MS Office, Antivirového SW a provozovaných IS a nástrojů pro správu systému.

Pro zajištění programové bezpečnosti je nezbytné:

* instalovat a aktualizovat programy pouze z důvěryhodných zdrojů pouze pověřenými zaměstnanci
* zajistit ochranu před škodlivým SW instalací spolehlivého antivirového prostředku, prostředku pro vyhledávání „spyware“ s automatickou aktualizací
* omezit poskytování síťových služeb pracovními stanicemi uživatelů a serverem instalací firewallu nebo vhodnou konfigurací operačního systému
* chránit lokální síť před neoprávněným přístupem z veřejných sítí - internetu, bezdrátových sítí (WiFi), atd.
* omezit přístupová práva uživatelů do IS a dat dle jejich pozice.
1. **Datová bezpečnost**

V případě ukládání dat na lokální disk odpovídá za poskytnutí vhodných prostředků pro řádné zabezpečení těchto dat proti možnosti zneužití (zabezpečení a omezení přístupu, antivir, firewall, …) jejich uživatel. Uživatel nemá právo tyto prostředky deaktivovat nebo měnit jejich nastavení nebo rozsah účinnosti.

V případě ukládání dat s osobními údaji je nutno u lokálního disku, pokud je to výkonově a technicky možné, nastavit režim šifrování disku, který znemožní případný nezákonný přístup k těmto OÚ.

V případě ukládání dat na disku serveru odpovídá za zabezpečení těchto dat správce ICT. Organizace mu poskytne potřebnou součinnost a prostředky k realizaci vhodných opatření.

Část IV. Realizace bezpečnostních opatření

1. **Pořizování, ukládání a zpracování dat**

Zpracováním dat se rozumí jakákoliv operace nebo soustava operací, které jsou systematicky prováděny s daty (vč. osobních údajů), bez ohledu na to, zda automatizovaně nebo jinými prostředky. Zejména se jedná o shromažďování, ukládání na nosiče informací, zpřístupňování, úpravu nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměnu, třídění nebo kombinování, blokování a likvidaci takových údajů.

Za obsahovou správnost, kompletnost a následné uložení dat v počítačové evidenci v okamžiku pořízení (změny) zodpovídá vždy ten, kdo data pořídil (změnil), bez ohledu na to, odkud byla data získána, a v čí pracovní náplni je sběr a zpracovaní těchto dat. Zaměstnanec, zadávající údaje do počítačové evidence, je povinen vždy si řádně ověřit věrohodnost a správnost těchto údajů. Zaměstnanec, který zjistí nesrovnalost mezi aktuálně zjištěným údajem a údajem v počítačové evidenci, je povinen tuto skutečnost neprodleně ohlásit příslušnému správci daného údaje a spolupodílet se na zajištění nápravy.

1. **Bezpečnost komunikačních cest**

Bezpečnost komunikačních cest se týká jednak zasílaných dat prostřednictvím počítačové sítě a jednak správy uživatelů.

Komunikační cesty jsou zabezpečeny vhodnými fyzickými prostředky (např. fyzicky chráničkami, v případě že procházejí v oblasti s trvalým přístupem veřejnosti, odpojením počítačových zásuvek od počítačové sítě v případě, že k zásuvce není připojen žádný prostředek ICT, …), aktivními a pasivními prvky sítě (router, firewall, switche,…), systémovými prostředky (SSH tunely, IPSec, AD, …) a aplikačními prostředky (monitorováním počítačové sítě, správa a omezení přístupu, …).

Pro komunikaci prostřednictvím internetu je preferován komunikační protokol HTTPS.

Pro datovou komunikaci se mimo provozované IS používá elektronická pošta a telefon. U těchto komunikačních cest organizace musí zabezpečit, aby e-maily, hovory, příp. uložené OÚ nemohly být zneužity.

1. **Ostraha budovy MěÚ**

Tato část směrnice určuje základní povinnosti zaměstnanců organizace při ochraně majetku budovy organizace.

Ostrahou majetku se rozumí souhrn přijatých opatření k zamezení vniknutí nepovolaných osob do objektů organizace, rozkrádání majetku a vzniku mimořádných situací.

1. **Mechanické zábranné prostředky a odpovědnost za jejich stav**

Mezi mechanické zábranné prostředky patří:

Oplocení objektu

* neporušenost oplocení objektu vizuálně kontrolují všichni zaměstnanci organizace a případné závady jsou povinni neprodleně hlásit tajemníkovi nebo jeho zástupci.

Uzamykací systém obvodové části objektu

* za uzamčení vstupních dveří a branek v mimopracovní době odpovídá provozní pracovník, popř. ten zaměstnanec nebo pracovník, který uzamyká budovu po skončení pracovní doby,
* elektronický zabezpečovací systém všech budov, za jehož aktivaci odpovídá pracovník nebo zaměstnanec, který uzamyká budovu po skončení pracovní doby a odchází z budovy jako poslední.

Uzamykací systém uvnitř objektu

* za uzamčení kanceláře odpovídá zaměstnanec odcházející jako poslední z kanceláře
* za uzamčení dveří do chodby, na kterou navazují kanceláře, odpovídá zaměstnanec odcházející jako poslední z kanceláří navazujících na tuto chodbu. V rámci úřadu se jedná o:
* u budovy č.p. 300 na Horním náměstí v Humpolci dveře navazující na chodbu, ze které je přístup do kanceláří Odboru dopravy a silničního hospodářství,
* spojovací dveře mezi budovami č.p. 301 a č.p. 300 na Horním náměstí v Humpolci,
* uzamykání šuplíků a skříní,
* trezory a pokladny v budově jsou umístěny mimo volně dostupných míst a za jejich řádné zabezpečení odpovídají příslušní zaměstnanci, kteří mají uzavřenu dohodu o odpovědnosti k ochraně hodnot svěřených zaměstnancům k vyúčtování.

Zabezpečení provozuschopnosti mechanických zábranných systémů zajišťuje tajemník.

1. **Způsob zabezpečení ochrany majetku**

Vstup do budovy organizace je povolen:

zaměstnancům organizace v pracovních dnech v čase volitelné pracovní doby:

* pondělí a středa v čase od 6:00 do 18:00 hod.
* úterý a čtvrtek v čase od 6:00 do 15.30 hod.
* v pátek v čase od 6:00 do 14:30 hod.

Mimo takto stanovenou dobu je vstup povolen pouze v případě plnění naléhavých pracovních povinností v souladu s pracovní smlouvou (krizové řízení, svatební obřady, výkony OSPOD apod.), pracovníkům a zaměstnancům dodavatelských společností v doprovodu pověřeného zaměstnance organizace v případě provádění úklidových a opravářských prací samostatně se svolením tajemníka MěÚ.

Výjimky povoluje tajemník organizace.

1. **Manipulace s klíči**
* Všechny klíče od vstupních branek, vchodů a dveří místností objektu jsou opatřeny příslušným označením.
* Za písemnou evidenci předání duplikátů klíčů od budovy a místností odpovídá pověřený zaměstnanec Odboru tajemníka MěÚ.
* Originály a duplikáty všech nerozdělených klíčů jsou uloženy v uzamčené plechové skříni v kanceláři sekretariátu Odboru tajemníka MěÚ, kam má přístup pověřený zaměstnanec sekretariátu Odboru tajemníka MěÚ. Tento odpovědný zaměstnanec vede evidenci celkového počtu vyhotovených klíčů od jednotlivých zámků a evidenci vydaných klíčů.
* Zaměstnanci přebírají klíče na základě písemného protokolu. V rámci předání je předávající seznámí s prostorami, od kterých klíče přebírají.
* Ztrátu klíčů je zaměstnanec povinen neprodleně hlásit tajemníkovi nebo jím pověřenému zaměstnanci, kteří rozhodnou o dalším postupu.
* Pro zaměstnance organizace, kterým jsou svěřeny klíče, je stanoven zákaz půjčovat klíče jiným osobám.
* Klíče od hlavního vchodu mají pověření zaměstnanci organizace dle systemizace klíčů a zámků v jednotlivých budovách úřadu. Výdej klíčů je na základě písemného požadavku nadřízeného zaměstnance.
* Klíče od prostorů s hmotnou odpovědností (dohoda o odpovědnosti k ochraně hodnot svěřených zaměstnanci k vyúčtování) a kanceláře zaměstnance Krizového řízení jsou ponechány pouze odpovědným zaměstnancům. V případě havárie jsou duplikáty klíčů uloženy v kanceláři sekretariátu Odboru tajemníka MěÚ v zapečetěných obálkách.
* V případě ztráty klíče od prostorů s hmotnou odpovědností je nutné vyměnit zámkový mechanismus, náklady spojené s výměnou zámkového mechanismu a vytvořením potřebného množství klíčů hradí zaměstnanec, který klíč ztratil.
1. **Režim zabezpečení budovy**

Vstup do budovy je povolen v provozní době zařízení, tj. v pracovní dny:

* pondělí a středa v čase od 6:00 do 18:00 hod.,
* úterý a čtvrtek v čase od 6:00 do 15:30 hod.,
* pátek v čase od 6:00 do 14:30 hod.

Vstup nebo pobyt zaměstnanců v budově mimo pracovní dobu (pracovní dny po 19:00 hodině a ve dnech pracovního klidu) musí být nahlášen tajemníkovi a zaznamenán do evidence docházky příslušného zaměstnance.

1. **Režim odemykání a uzamykání dveří**

Uzamykání hlavních vchodových dveří

* Za uzamčení vchodových dveří odpovídá každý pracovník nebo zaměstnanec, odcházející po provozní době z úřadu v případě, že budou vchodové dveře v době odchodu již uzamčeny.

Uzamykání dveří v budově organizace

* Za uzamčení dveří od kanceláří odpovídá poslední zaměstnanec, který z kanceláře odchází.
1. **Identifikační čipy**

Zaměstnanci používají čipy pro evidenci jak při příchodu, tak při odchodu z budovy s uvedením důvodu odchodu označením na Docházkovém terminále.

1. **Elektronické zabezpečení budovy**

Budova je zajištěna elektronickým zabezpečovacím systémem (EZS), provozovaným firmou JABLOTRON SECURITY a.s., Praha 4 Chodov, který je napojen na centrální pult provozovaný touto společností a je zapnut bezprostředně po odchodu zaměstnanců úřadu, popř. provozních pracovníků zabezpečující úklid a údržbu objektů.

Elektronický zabezpečovací systém má výstup na pult centrální ochrany smluvně provozovaný bezpečnostní agenturou, která bezprostředně kontaktuje pověřené provozní pracovníky úřadu, popř. tajemníka MěÚ a zároveň dle jejich pokynů vysílá asistenční službu ke kontrole střežených objektů.

Popis systému a technické podrobnosti jsou uloženy u smluvního provozního pracovníka a tajemníka MěÚ.

Ovládací klávesnice jsou umístěny za vchodovými dveřmi budovy.

Zaměstnanci oprávnění k aktivaci a deaktivaci zabezpečovacího poplašného systému mají přiděleny kódy, které jim poskytují přístupová práva k systému. Přístupová práva nejvyšší priority, která umožňují přidělovat a diferencovat přístupová práva dalších osob má pouze na základě pokynu tajemníka MěÚ pověřený pracovník provozovatele EZS.

V případě poplachu zabezpečovacího zařízení obsluhou omylem (např. při nezadání kódu v maximálním povoleném čase), jsou oprávnění zaměstnanci poučeni o dalším postupu (deaktivaci poplachu).

Vchody organizace jsou opatřeny informačními nálepkami o zajištění budovy zabezpečovacím zařízením.

Po ukončení pracovního poměru (případně jiného právního vztahu) na základě informace od nadřízeného zaměstnance zablokuje správce systému do druhého pracovního dne, ve zdůvodněných případech nejpozději do 3 pracovních dnů přístup do budovy na základě kódu zaměstnance, kterému skončil pracovní poměr nebo jiný obdobný smluvní vztah.

1. **Zabezpečení majetku organizace**

Pojištění budovy zajišťuje dle zřizovací listiny Odbor tajemníka MěÚ ve spolupráci s Ekonomickým odborem. Majetek organizace je pojištěn prostřednictvím společnosti ADORES, centrum pojištění s.r.o., Humpolec IČO 26049864, přílohou pojistné smlouvy jsou pojistné podmínky, které stanovují požadavky na zabezpečení – typy zámků, zámkových vložek, ochranných folií apod. Při opravách je nutné se řídit těmito požadavky.

Pro přebírání majetku dodaného organizaci, jeho řádnou evidenci a správu jsou organizací vydány vnitřní směrnice (předpisy) upravující zejména oběh účetních dokladů, odpisování dlouhodobého majetku, provedení inventarizace.

Zaměstnanec, který odchází z příslušného pracoviště jako poslední, je povinen:

* překontrolovat uzavření všech oken,
* překontrolovat vypnutí světel a elektrospotřebičů,
* překontrolovat, že jsou řádně uzavřené vodovodní kohoutky a neprotéká WC,
* uschovat cenné věci na jednotlivých pracovištích na určené místo,
* zamknout vstupní dveře na své pracoviště a klíče z určených pracovišť uložit na smluvené místo,
* pracovník nebo zaměstnanec, který odchází z budovy jako poslední, překontroluje uzamčení všech vstupních dveří do budovy, překontroluje, že už se v budově nikdo nenachází, uzamkne vstupní dveře a aktivuje prvky EZS,
* pokud nejdou z jakéhokoliv důvodu zamknout vstupy do budovy, nesmí pracovník nebo zaměstnanec, který odchází jako poslední odejít, je povinen nahlásit situaci přímému nadřízenému nebo tajemníkovi,
* zaměstnanci jsou povinni oznamovat svému nadřízenému nedostatky, závady a rizika, které by mohly vést ke vzniku škody na majetku organizace a podle svých možností se účastnit na jejich odstraňování. Na hrozící škodu je zaměstnanec povinen upozornit tajemníka a přispět k jejímu odvrácení.
1. **Zabezpečení finanční hotovosti**

Peněžní prostředky a ceniny jsou trvale uloženy pouze v trezoru odpovědného zaměstnance, nesmí překročit stanovený limit, který je stanoven s ohledem na technické podmínky zabezpečení a v souladu s podmínkami pojistné smlouvy a je uveden v písemné podobě. Limit vychází z pojistných podmínek pojišťovny, které stanoví úroveň zabezpečení a z úrovně technického vybavení.

Přeprava finanční hotovosti z banky a do banky probíhá v souladu s podmínkami pojistné smlouvy, která určuje s ohledem na výši přepravované částky počet osob zajišťujících přepravu a způsob zabezpečení. Peníze jsou přepravovány v uzamykatelné tašce, bezpečnostním kufříku vždy v pracovní době.

Výplata platů zaměstnancům organizace probíhá bankovním převodem na soukromé číslo účtu zaměstnance.

Hotovostní platby jsou co nejvíce omezeny. Úhrady za stravné jsou realizovány hotovostním převodem.

Dohody o odpovědnosti k ochraně hodnot svěřených zaměstnanci k vyúčtování jsou uzavřeny na odpovědnost za hotovost v pokladnách i drobný hmotný majetek vždy s konkrétním zaměstnancem.

1. **Zabezpečení majetku zaměstnanců organizace**

Se způsoby zabezpečení osobního majetku a povinnostmi, které z nich vyplývají, jsou zaměstnanci organizace seznámeni každoročně prokazatelným (písemným) způsobem.

O škodě vzniklé zaměstnanci musí zaměstnanec uvědomit bez zbytečného odkladu zaměstnavatele, nejpozději ve lhůtě do 24 hod. od zjištění škody.

Věci, které do zaměstnání obvykle zaměstnanci nenosí (větší částky peněz, klenoty a jiné cennosti) je možné během dne uložit do trezoru organizace. Věci, které zaměstnanec odložil při plnění pracovních úkolů nebo v přímé souvislosti s ním, musí být uloženy na místě k tomu určeném.

Ve všech prostorách organizace platí zákaz ponechávat peníze v hotovosti a osobní cenné věci volně nezabezpečené ve stolech nebo skříních a ponechávat je takto nezajištěné v organizaci přes noc.

1. **Zabezpečení počítačových dat**

Ochrana dat

* Smyslem ochrany dat je učinit taková organizační a technická opatření, která v nejvyšší možné míře omezí možnost nenávratného poškození nebo ztráty dat, minimalizují negativní dopady, způsobené poškozením nebo ztrátou dat, na další činnost organizace. Přijatá opatření zamezí v přístupu k datům nepovolaným osobám.
* Předmětem ochrany jsou veškerá programová vybavení včetně doprovodné dokumentace, všechna provozní data uložená na nosičích informací, v paměti počítačů, tiskáren a dalších zařízení výpočetní techniky, záložní a archivní kopie dat uložené na nosičích informací, údaje zobrazené nebo vytištěné na výstupních zařízeních; přístupová hesla, technické informace o informačním systému a návody.
* Všichni zaměstnanci, přicházející do styku s výpočetní technikou, jsou povinni učinit a průběžně dodržovat taková bezpečnostní opatření, která v maximální možné míře vyloučí nenávratnou ztrátu a trvalé poškození provozních dat, která by mohla být způsobena náhodným nebo úmyslným zásahem další osoby, neodbornou obsluhou, poruchou výpočetní techniky, požárem, živelní pohromou, atp.
* Mezi způsoby ochrany patří zejména znemožnění jakéhokoli přístupu nepovolaných osob k výpočetní technice a datům, a to jak v pracovní, tak i v mimopracovní době. Neponechávání zapnuté techniky bez dozoru. Situování pracoviště tak, aby nebylo možno odečítat údaje z monitorů nepovolanými osobami. Uložení tiskových výstupů mimo dosah nepovolaných osob. Ochrana přístupovým heslem, udržování hesla v tajnosti, změna hesla. Heslo je tvořeno znaky, může obsahovat kombinaci číslic, malých a velkých písmen, nebo speciálních znaků. Důsledné odhlašování se při delší nepřítomnosti na pracovišti. Není dovoleno přesunovat, odpojovat, přenášet, připojovat a ani jinak manipulovat s umístěným zařízením bez předchozí domluvy se správcem IT nebo nadřízeným zaměstnance.

Způsob zabezpečení přístupu v rámci jednotlivých typů zařízení

|  |  |
| --- | --- |
| **Technologie** | **Způsob zabezpečení přístupu** |
| Počítačová síť | Přihlášení k aktivním prvkům sítě: login + heslo (ne defaultní)Segmentace sítě v rámci možností stávajících technologiíVypnutí nepoužitých zásuvekMonitoring přístupu na úrovni aktivních prvků sítě |
| Server | Přihlášení: Login+hesloMonitoring přístupuNastavení automatického uzamčení při nečinnosti zaměstnance  |
| PC | Přihlášení: Login+heslo (autentizace i do počítačové sítě)Nastavení automatického uzamčení při nečinnosti zaměstnance delší jak 15 minut |
| Notebook | Přihlášení: Login+heslo (autentizace i do počítačové sítě)Nastavení automatického uzamčení při nečinnosti zaměstnance delší jak 15 minutV případě, že se využívá i mimo budovu organizace a na disku jsou ukládány osobní údaje, nastavení šifrování dat na úrovni disku správcem IT, pokud je toto nastavení z výkonových důvodů možné. |
| Externí média s OÚ (flash disk,..) | Omezení využití pouze na povolená pracoviště po schválení nadřízeným zaměstnance.Přihlášení: Heslo (šifrování dat na úrovni flash disku) v případě, že jsou na flash disk ukládány osobní údaje. |
| Mobilní telefon s OÚ(soukromý i firemní) | Přihlášení: heslem nebo obdobnou technologiíNastaveno automatické uzamykání mobilu v případě nečinnosti Přístup k SIM kartě vázán na PIN  |
| Sdílené disky | Segmentace na úrovni:* organizace
* odbor
* oddělení
* uživatel

Každý má přístup pouze k vlastnímu uživ. segmentu. Přístup k ostatním segmentům určuje nadřízený zaměstnance, nastavuje správce IT |
| IS | Přihlášení: login + heslo (příp. s vazbou na AD/LDAP), certifikátem (podle podpory daným IS)Monitoring přístupu k OÚ |
| Pravidla pro generování hesel | Min. 8 znakůMin. 1 čísloMin. 1 malé písmeno a 1 velké písmenoNa server, nebo PC s citlivými daty – min. 1 speciální znak (čárka, lomítko, zavináč, apod.)Heslo musí obsahovat bezvýznamovou kombinaci alfanumerických znaků. V případě zvýšených nároků na bezpečnost dat, může správce ICT zpřísnit pravidla pro tvorbu hesel a přihlašování (uložit provádění pravidelné změny hesla, změnit minimální počet znaků, pokusů přihlášení apod.). |

Zálohování a archivace dat

* Za zálohování provozních dat, uložených na pevných discích počítačů odpovídá uživatel ICT.
* Ukládání dat velkých objemů (nad cca 10 GB) je uživatel povinen konzultovat se správcem ICT. Správce ICT je oprávněn limitovat uživateli dostupné místo na síťových serverech, aby zajistil jejich plynulý chod.
* Za zálohování provozních dat, uložených na serverech odpovídá správce ICT. Data jsou zálohována automaticky, a to ze všech serverů, které jsou přihlášeny do počítačové sítě. Plná záloha (ne přírůstková) se provádí 1x týdně. Každý den jsou v nočních hodinách prováděny denní inkrementální (přírůstkové) zálohy. Záloha a archivace je prováděna denně na externí úložiště.
* Záložní kopie dat jsou uloženy mimo místnost, kde se počítač nachází – ideálně v jiné budově, pokud to není technicky možné, fyzicky v jiné části budovy.
* V případě, že záložní kopie obsahují osobní údaje, jsou uloženy v zašifrované podobě, příp. pod heslem.

Část V. Zásady pro práci s výpočetní technikou

**Zásady pro práci s výpočetní technikou**

* Na počítačích mohou pracovat pouze zaměstnanci k tomu pověření. Prostředky, na kterých jsou zpracovávány osobní údaje, chrání příslušní zaměstnanci před neoprávněným přístupem přístupovými hesly, nebo obdobným bezpečnostním opatřením (otiskem prstu, PINem, apod.).
* Každému uživateli správce ICT přidělí na serveru příp. počítači jedinečný uživatelský účet (2 zaměstnanci organizace nesmí mít jeden uživatelský účet). Přidělením uživatelského účtu správce IS uživateli povoluje přístup k uživatelským programům serveru/počítače. Uživatel získá přístup k uživatelským programům a datům, které vyplývají z jeho pracovní náplně a musí dbát ochrany dat ve smyslu GDPR a zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.
* Správce informačního systému přidělí uživateli uživatelské jméno a počáteční přístupové heslo. Počáteční nastavené heslo nebo implicitní heslo musí být uživatelem při prvním přihlášení změněno. Uživatel je povinen si své uživatelské heslo udržovat v tajnosti. V případě zapomenutí hesla oznamuje uživatel tuto skutečnost správci ICT, který mu přidělí nové počáteční heslo.
* Přihlášení do počítače je možné i pod administrátorským účtem, jehož heslo zná správce ICT. Všechny požadavky na nákup programového vybavení a spotřebního materiálu schvaluje nadřízený správce ICT.
* Na počítačích organizace je používán antivirový program, který je nastaven tak, aby jeho aktualizace byly prováděny automaticky prostřednictvím internetu. Bez svolení správce ICT nesmí uživatel měnit nastavení nebo vypnout ochranu antivirovým programem a firewallem.
* Kromě statistických sledování a hlášení nadřízeným orgánům je zakázáno poskytovat přes internet údaje o organizaci a zaměstnancích.
* Je zakázáno používat nelegální software; používat software, jehož použití nebylo schváleno správcem ICT, instalovat bez svolení správce ICT na disky počítačů jakýkoliv software či data s tímto programovým vybavením související, odstraňovat instalovaný software, provádět změny v nastavení a umístění software a souvisejících dat, pořizovat kopie software a dat pro jinou, než služební potřebu, předávat data jiným subjektům bez předchozího souhlasu příslušného nadřízeného zaměstnance, provádět demontáž, úpravy, opravy, změny v nastavení a zapojení prostředků ICT, používat prostředky ICT pro jiné, než schválené účely, instalovat a hrát počítačové hry.
* Na základě ustanovení § 32 zákona č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů, se doklady osvědčující legální nabytí software uchovávají po celou dobu užívání licence, není možné je skartovat spolu s ostatními doklady v účetnictví. Z tohoto důvodu správce ICT vede v součinnosti s účetní organizace, evidenci všech typů licencí s odkazy na účetní doklady a evidenci umístění instalačních médií a souvisejících tiskovin – manuálů, ve kterých může být zaznamenán počet licencí, datum aktivace, datum vypršení licence a další informace.

**Práva a povinnosti zaměstnance – uživatele ICT**

* Odpovídá za bezpečnost dat uložených na lokálním počítači.
* Při krátkodobém opuštění pracoviště (do 30 min.) uzamknout PC klávesami CTRL+ALT+DEL a volbou „Uzamknout“ nebo Windows klávesa s logem+L. Při dlouhodobém opuštění pracoviště (déle než 30 min.) nebo ukončení pracovní doby ukončit veškerý spuštěný SW a PC vypnout.
* Řídí se pokyny správce ICT nebo provozovaného IS.
* Při zahájení práce s ICT je zaměstnanec povinen překontrolovat stav a kompletnost svěřených prostředků výpočetní techniky. Ukončování činnosti programů se provádí předepsaným způsobem, včetně ukončení práce v počítačové síti. Před odchodem zaměstnance z pracoviště musí být všechny jemu svěřené prostředky, tj. osobní počítače, tiskárny atd., vypnuty, s výjimkou těch zařízení, která musí zůstat s ohledem na své určení trvale zapnuta.
* Zaměstnanci jsou povinni zachovávat mlčenlivost vůči třetím osobám ve smyslu GDPR a o zjištěných údajích, se kterými v rozsahu svých oprávnění přicházejí do styku včetně bezpečnostních incidentů a nedostatků.
* Každý uživatel smí užívat přidělený uživatelský účet výlučně pro vlastní potřebu. Získané údaje (zejména heslo) nesmí sdělovat neoprávněným osobám. V případě, že uživatel tyto údaje sdělí neoprávněným osobám je zodpovědný za škody, které budou způsobeny zneužitím jeho uživatelského účtu. V případě, že zjistí přístupové heslo jiného uživatele, nebo se dostane k prostředku, kde je jiný uživatel přihlášen, nebo jeho datům, které nevhodně uložil, nesmí zneužívat této nedbalosti jiného uživatele. Takovouto skutečnost je povinen nahlásit.
* Jakoukoli závadu nebo i podezření na nestandardní fungování počítače, nebo nově zjištěná bezpečnostní rizika a incidenty, podezřelé zprávy, zaměstnanec bez zbytečného odkladu hlásí svému nadřízenému nebo pověřenému zaměstnanci správou ICT. Do odstranění závady nebo prověření nezávadného stavu nesmí zaměstnanci používat technické zařízení v síti (např. v systému elektronického bankovnictví). V případě podezření na virovou nákazu je uživatel povinen se neprodleně odhlásit od počítačové sítě a ohlásit tuto událost správci ICT.
* Udržovat přidělené technické vybavení v čistotě a provádět základní pravidelnou údržbu od prachu a nečistot.
* Užívat informační a komunikační technologie pouze k plnění svých pracovních povinností a v souladu s účelem, ke kterému byly určeny. Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.
* Vyskytne-li se potřeba provést určité opravy či aktualizace počítačových programů nebo výpočetní techniky, oznámit tuto skutečnost správci ICT, nebo nadřízenému zaměstnance.
* Odpovídá za případné škody způsobené jím rozšířenými počítačovými viry, např. při manipulaci s přenosnými datovými médii, s elektronickou poštou, mobilními prostředky.
* Nesmí vytvářet nebo pozměňovat data s cílem ovlivnit (zmást) kontrolu oprávněnosti použití počítačových programů.
* Znemožňovat nebo přerušovat funkci ochranného SW (antivir, …).
* Software, který je součástí IS organizace může používat pouze v souladu s licenčními podmínkami pro daný typ počítačových programů.
* Tiskové výstupy obsahující data podléhající ochraně osobních údajů musí příslušný zaměstnanec zabezpečit před neoprávněným přístupem.
* Je zakázáno připojovat uživatelům do počítačové sítě další zařízení (mobilní, vlastní) bez souhlasu správce ICT nebo nadřízeného zaměstnance.
* Je zakázáno obtěžovat ostatní uživatele rozesíláním hromadných zpráv, např. pro šíření obchodních nebo marketingových informací, pro politickou nebo náboženskou agitaci a pro šíření materiálu, které mohou poškodit jméno organizace, nebo jsou v rozporu s právními předpisy.
* V případě zasílání osobních údajů na mailové adresy veřejných provozovatelů (gmail.com, seznam.cz, apod.) údaje s osobními údaji zazipovat pod heslem do přílohy a heslo sdělit adresátovi jinou cestou.
* V případě rozesílání hromadných mailů vně organizace, uvádět adresáty ve skryté kopii, aby navzájem neviděli mailové adresy ostatních adresátů. Výjimku tvoří maily právním subjektům, které se navzájem vyjadřují/připomínkují k dané věci.
* Při nepřítomnosti (nemoc, dovolená) zapnout, nastavit v outlooku funkci „mimo kancelář“.
* V případě jakýchkoli problémů, potíží je zaměstnanec povinen kontaktovat zástupce IT v tomto pořadí:
	+ prostřednictvím helpdesku (http://intranet/helpdesk/)
	+ emailem (it@mesto-humpolec.cz)
	+ telefonicky (linka 121 a 125).

**Práva a povinnosti personalisty organizace a nadřízeného zaměstnance**

* Personalista neprodleně předává správci ICT informaci o nástupu nového zaměstnance, změně pracovního zařazení, nebo obsahu práce.
* Nadřízený zaměstnanec předává správci ICT informaci o přístupových právech zaměstnance k IS, nebo jejich změnách a o ukončení nebo přerušení pracovního poměru zaměstnance.

**Práva a povinnosti správce ICT**

* Zajišťuje přístup všem oprávněným uživatelům IS k uživatelským programům (instalovaných na klientských počítačích nebo serverech) v provozních hodinách.
* Zajišťuje školení nových uživatelů.
* Zajišťuje komunikaci s dodavatelem IS.
* Uživatelé IS mu předávají informace o chybách, námětech a legislativních požadavcích na IS.
* Zajišťuje bezporuchový provoz klientských počítačů, datové sítě a serverů.
* Odpovídá za bezpečnost, zálohování a obnovitelnost dat ze záloh na serverech.
* Zajišťuje ochranu všech datových souborů programového vybavení uložených na serveru před zneužitím, poškozením, ztrátou a zničením.
* Provádí činnosti související s konfigurací sítě a administrací síťového operačního systému (instalace a úpravy v systému, změny v prostředí systému, instalace a konfigurace doplňkových programů, spolupráce s dodavateli uživatelských programů v prostředí síťového operačního systému).
* Provádí činnosti související s technickou správou klientských počítačů sítě (instalace a konfigurace programového vybavení na klientských počítačích).
* Provádí administraci uživatelských účtů. Zajišťuje přístup oprávněných uživatelů k uživatelským programům, pokud jim tento přístup byl povolen.
* Dohlíží na dodržování této směrnice všemi uživateli v oblasti IT.
* V případě výskytu závady na některém serveru nebo klientském počítači tuto závadu identifikuje a zajistí její odstranění, případně zajistí náhradní provoz.
* Zablokuje proti neoprávněnému přístupu uživatelský účet zaměstnance – uživatele informačního systému, který ukončil pracovní poměr.
* Informuje uživatele IS o změnách programového vybavení, jeho ovládání a instalaci nového softwaru.
* Vydává pokyny uživatelům související s provozem operačního systému a sítě, zejména v případě výskytu závady na serveru a vyžaduje jejich plnění.
* Odepře přístup k službám serveru těm uživatelům, kteří porušují tuto směrnici nebo nedodržují jeho pokyny. K odepření přístupu správce používá nástrojů administrace uživatelských účtů. O odepření přístupu neprodleně informuje nadřízeného zaměstnance.
* Stanoví režim pravidelné archivace dat.
* Při skončení nebo změně pracovně právního nebo obdobného vztahu správce ICT provede úpravu (případné odstranění) uživatelského účtu zaměstnance, včetně přístupových práv.

Část VI. Kontrolní mechanismy

Správce ICT je oprávněn v rámci své kompetence monitorovat vytížení počítačové sítě a oprávněnost využívání jednotlivými uživateli.

Správce ICT vede přehled o instalaci software na jednotlivé pracovní stanice a provádí průběžnou kontrolu. Jakékoli porušení této směrnice hlásí svému nadřízenému.

Zaměstnanec v pozici vedoucího zaměstnance periodicky i nahodile kontroluje u svých podřízených dodržování této směrnice a z realizovaných kontrol provádí zápis.

Pověřený zaměstnanec organizace provádí periodickou i nahodilou kontrolu činností zpracovávajících osobní údaje elektronickou formou. Z prováděných kontrol je vyhotoven zápis.

Pověřený zaměstnanec provádí periodickou nebo nahodilou kontrolu (min. 1x ročně) souladu zabezpečení dat s GDPR u jednotlivých zpracovatelů OÚ.

Provozní hodiny počítačové sítě a serverů jsou stanoveny takto:

Po 06:30-18:00
ÚT 06:30-18:00
ST 06:30-18:00
ČT 06:30-18:00
PÁ 06:30-15:00
V případě mimořádných událostí může být výše uvedený čas upraven. Doba mimo tyto hodiny, je vyhrazena pro servis (zálohování, údržbu apod.).

Část VII. Závěrečná a přechodná ustanovení

* + - 1. Tato směrnice byla schválená na 18. schůzi Rady města Humpolec dne
			13. září 2023 pod číslem usnesení xx/18/RM/2023 a nabývá účinnosti dne
			1. října 2023.
			2. Touto směrnicí se zrušuje směrnice č. 1/2008, kterou se stanoví pravidla pro ochranu majetku města v objektech Městského úřadu Humpolec ze dne
			1. ledna 2008 a Bezpečnostní směrnici č. 1/2018 ze dne 6. června 2018.

V Humpolci, 13. září 2023

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mgr. Alena Štěrbová, starostka města Mgr. Jiří Fiala, tajemník MěÚ