Bezpečnostní politika městského úřadu Jáchymov

Leden 2023

Obsah

1. ÚVOD

Bezpečnostní politika Městského úřadu Jáchymov (dále jen „Bezpečnostní politika“) představuje ochranu informací ve všech jejich formách, po celý jejich životní cyklus – tedy během jejich vzniku, zpracování, ukládání, přenosu a likvidace.

1.1 Účel dokumentu

Účelem tohoto dokumentu je stanovení bezpečnostní politiky Městského úřadu Jáchymov.

1.2 Určení a platnost

Dokument je určen pro vnitřní potřebu MěÚ Jáchymov. Tento dokument formuluje bezpečnostní politiku, a proto je platný pro všechny zaměstnance úřadu, volené zástupce města a jemu podřízených institucí bez ohledu na to, zda pro svou práci informační technologie využívají nebo ne.

1.3 Formulace a vymezení působnosti bezpečnostní politiky

Dokument se nevztahuje na ty podřízené organizace, které využívají dat uložených v informačním systému úřadu prostřednictvím dálkového přístupu se stupněm oprávnění shodným s veřejností (např. využití veřejně přístupných informací z webových stránek úřadu.).

1.4 Cíl bezpečnostní politiky

Cílem této politiky je zajistit bezpečnost informačního systému proti všem hrozbám narušení bezpečnosti informací. Pro ochranu informací jsou důležitá tři zásadní hlediska:

- Zajištění důvěrnosti, tj. chránit informaci proti tomu, kdo k ní nemá přístup
- Zajištění integrity, tj. chránit informaci před úmyslnou či náhodnou modifikací a zajistit správnost a úplnost informace
- Zajištění dostupnosti, tj. zajistit, aby informace byla dostupná vždy tomu, kdo k ní má mít přístup

1.5 Definice informace

Veřejná	Informace veřejně známá, nepodléhající žádné ochraně
Interní	Informace neveřejného charakteru, které mohou být bez vážných následků zpřístupněny všem zaměstnancům. Zařazení informace do této třídy však nedává každému zaměstnanci nárok, aby mu byla informace zpřístupněna.
Striktně interní	Informace se zásadním významem, které jsou přístupné pouze omezenému okruhu osob a dalším subjektům mohou být předávány jen za dodržení zvláštních podmínek stanovených bezpečnostní politikou.
Osobní údaje	Osobní údaje a citlivé osobní údaje ve smyslu zákona 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů a v souladu s GDPR
Zvláštní skutečnosti	Informace ve smyslu zákona 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.
Utajované skutečnosti	Skutečnosti utajované podle zákona 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozd. předpisů. Zajištění jejich ochrany je řešeno zvláštním předpisem.

1.6 Aktuálnost

Aktuálnost tohoto dokumentu kontroluje zpracovatel nejméně jednou ročně.

1.7 Použité pojmy

Auditní záznam
Záznam o událostech, které mohou ovlivnit bezpečnost informačního systému

Důvěrnost dat
Zajištění toho, že k informaci má přístup pouze ten, kdo byl autorizován k přístupu

E-learning
Vzdělávací proces, využívající informační a komunikační technologie k tvorbě kurzů, k distribuci studijního obsahu, komunikaci mezi studenty a pedagogy a k řízení studia

GDPR
Obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation, zkratka GDPR), plným názvem nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), je nařízení Evropské unie, jehož cílem je výrazné zvýšení ochrany osobních dat občanů

HW (Hardware)
Veškeré fyzicky existující technické vybavení – počítače, tiskárny, skenery, monitory, mobilní telefony, přenosná média a jiné.

Informační systém
Celek složený z počítačového hardwaru a souvisejícího softwaru, k němuž patří také lidé, kteří tento hardware a software využívají, a procesy (činnosti), které přitom vykonávají za účelem sběru, zpracování a šíření informací potřebných k plánování, rozhodování a řízení

Informace
V nejobecnějším smyslu je informace chápána jako údaj o prostředí, jeho stavu a procesech v něm probíhajících. Informace snižuje nebo odstraňuje neurčitost (entropii) systému (např. příjemce / uživatele informace). Množství informace lze charakterizovat tím, jak se jejím přijetím změnila míra neurčitosti přijímajícího systému

Integrita dat
Stav, kdy přečtená data jsou totožná s daty uloženými. Tzn. během uložení (přenosu) dat nedošlo k jejich neočekávaným změnám

Login
V počítačové terminologii označuje proces přihlášení k účtu (tedy autentizaci) pomocí uživatelského jména a zpravidla hesla nebo certifikátu

Monitoring
Monitoring je sběr informací probíhající systematicky a po určitou dobu

PC
Personal computer, počítač

SW (Software)
Software je v informatice sada všech počítačových programů používaných v počítači, které provádějí nějakou činnost. Software lze rozdělit na systémový software, který zajišťuje chod samotného počítače a jeho styk s okolím a na aplikační software, se kterým buď pracuje uživatel počítače nebo zajišťuje řízení nějakého stroje.

Home office
Home Office je anglický pojem pro možnost pracovat z domova. Home Office patří mezi často používaný zaměstnanecký benefit.

ZOZ
Zvláštní odborná způsobilost

VPN
Virtuální privátní síť (zkratka VPN, anglicky virtual private network) je v informatice prostředek k propojení několika počítačů prostřednictvím nedůvěryhodné počítačové sítě (např. veřejný Internet). Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy většinou důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné

Active Directory
V informatice název adresářových služeb LDAP implementované firmou Microsoft. Adresářová služba Active Directory je rozšiřitelná a škálovatelná adresářová služba, která umožnuje efektivně uspořádat sítové prostředky

Microsoft Exchange Server
Softwarový produkt společnosti Microsoft, který slouží k výměně e-mailových zpráv a sdílení zdrojů

Token
Fyzické zařízení, které usnadňuje uživatelům zabezpečených služeb ověření pro přístup a užívání. Bezpečnostní tokeny se používají pro ověření identity uživatele elektronickou cestou (tokeny obsahují elektronické certifikáty). Token se používá namísto hesla nebo jako doplněk k ověření, že uživatel je tím, za koho se vydává. Token je tedy elektronický klíč, který lze využít v mnoha aplikacích.

2. OBECNÉ BEZPEČNOSTNÍ ZÁSADY

2.1 Ochrana duševního vlastnictví – programové vybavení

- Na počítačích musí být nainstalováno pouze legální programové vybavení.
- Bez souhlasu odpovědné osoby si žádný z uživatelů nesmí instalovat jakýkoliv software. Instalovaný SW bude využívaný pouze k plnění pracovních povinností.
- Zaměstnanci nesmí kopírovat programové vybavení v majetku úřadu.
- Je zakázáno kopírovat fotografie, videa a audio záznamy, které jsou v majetku úřadu.
- Sdílené skupinové adresáře, kalendáře apod. musí být chráněny odpovídajícím způsobem, aby nebyly prozrazeny informace.
- Při používání mobilních telefonů a notebooků na veřejných místech musí zaměstnanec zajistit, že nebude prozrazena žádná informace.
- Porušení tohoto odstavce bude postihováno dle kapitoly 9.3 tohoto dokumentu.

2.2 Ochrana majetku – hmotný majetek

- Notebooky, tablety, mobilní telefony apod. nesmí být nikdy ponechány v autě, pokud v něm nikdo není.
- Stejně tak nesmí být tato zařízení ponechána bez dozoru nikde ve veřejných dopravních prostředích, ani jiných veřejných místech.

- Zaměstnanci, kteří tato zařízení používají na veřejných místech, si musí být vědomi, že je možné je odposlouchávat, monitorovat komunikaci či odezírat z displeje a dle toho se musí zachovat.
- Všechny notebooky, tablety a mobily musí být zabezpečeny heslem, které zamezí vniknutí útočníka, rodinných příslušníků a nepovolaných osob do zařízení a tím ochrání data v zařízení.
- USB Flash disky musí být šifrovány a každý zaměstnanec bude mít vlastní zaměstnanecký USB Flash disk.
- V prostředí IS úřadu je dovoleno používat jen média schválená a evidovaná odpovědnou osobou. Všechna používaná média musí být pod kontrolou zaměstnanců úřadu, aby nemohlo dojít k jejich odcizení či neoprávněnému použití.
- Uživatel, který uložení informací provedl, je dále zodpovědný za ochranu informací, které na přenosné medium uložil. Na přenosná média nesmí být ukládány osobní nebo důvěrné informace, v případě nutnosti uložení takových informací, musí být před uložením zašifrovány.

2.3 E-mailová komunikace

- Pokud si zaměstnanec není jistým odesílatelem e-mailu, nesmí bez souhlasu informatiků:
    - Otevírat jakékoliv odkazy v e-mailu
    - Ukládat na pevný disk počítače jakýkoliv spustitelný soubor
    - Ukládat na pevný disk počítače jakýkoliv zazipovaný soubor
- Je zakázáno na pracovních PC využívat soukromých e-mailů, v případě zjištění porušení se bude postupovat dle kapitoly sankce

2.4 Sociální sítě a streamovací služby

- V pracovní době je zakázáno využívání sociálních sítí (Facebook, Twitter, Instagram, Pitnterest apod.)
- Stejně tak je zakázáno využívat video streamovacích portálů (Youtube, Stream.cz, Twitch apod.) a hudebních streamovacích portálů (Spotify, Amazon Musíc, Apple Music, Youtube Music apod.)

2.5 Internetové připojení

- Přístup na internetové stránky, které nesouvisí s výkonem práce úředníka, jsou standardně monitorovány.
- Výjimkou jsou vedoucí pracovníci a vedení úřadu a města nebo jimi pověření referenti.

2.6 Obecná opatření

- Při práci s kopírkami a tiskárnami, scannery je nutné, aby vytištěné, zpracované dokumenty nezůstaly v zařízení.
- Při odchodu z kanceláře je zaměstnanec povinen zabránit přístupu do kanceláře cizí osobě a to tím, že zamkne dveře.
- Zaměstnanci si musí být vědomi toho, že citlivé informace mohou být také prozrazeny při diskuzi ve veřejných dopravních prostředcích nebo na veřejných místech.
- V souladu s nařízením GDPR je nutné dodržovat následující zásady:
    - „Prázdný stůl“ – veškeré citlivé údaje je zaměstnanec povinen odstranit z viditelných míst (stůl, police) a umístit je do zavírací skříně. Přísně důvěrné informace a razítka jsou uloženy v uzamykatelném šuplíku, či skříni.
    - „Prázdná obrazovka“ – zaměstnanec je povinen zajistit, aby nepovolaná osoba neviděla údaje, které nejsou předmětem jednání
- Zaměstnanec je povinen při opuštění pracoviště vypnout počítač – povolenou výjimkou jsou oprávněné osoby a pověření zaměstnanci z důvodu HomeOffice.
- Zaměstnanec nesmí žádné další osobě sdělit přístupové heslo k počítači, poskytovat klíče zaměstnancům, kteří v kanceláři nepracují, nebo je v kanceláři ponechávat bez dozoru.
- Zastupitelnost pracovníka nesmí být řešena sdělováním hesla.
- Z důvodu zajištění bezpečnosti musí zaměstnanec kdykoliv umožnit informatikovi přístup na jeho PC

- PC musí odolat tzv. offline útokům
  - Uživatel si nesmí ukládat hesla do prohlížeče
  - Při odchodu od PC je zaměstnanec povinen zamezit cizímu přístupu uzamčením počítače.
    - Standardně je nastaveno zamčení PC po 15 minutách nečinnosti.
  - Přístupová hesla nesmí být napsána v kalendářích, nalepená na monitorech apod.

3. ORGANIZACE BEZPEČNOSTI

3.1 Role uživatelů informačních systémů

3.1.1 Uživatel aplikace

Má k aplikaci přidělen login s oprávněním odpovídajícím jeho pracovní náplni. Buď je oprávněn zadávat a měnit data, nebo má oprávnění pouze k prohlížení. Uživatel je odpovědný za utajení svého přístupového hesla. Je povinen vždy okamžitě po ukončení práce s aplikací se odhlásit.

3.1.2 Správce aplikace

Správce aplikace je uživatel aplikace, kterému byla přidělena práva měnit oprávnění ostatních uživatelů aplikace a/nebo měnit nastavení aplikace.

3.1.3 Informatik/oprávněná osoba

Informatik disponuje plným přístupem na všechny síťové i lokální disky. Rozhoduje o přidělení a změně uživatelských práv, každá změna v právech bude zapsána do Evidence práv. Evidence práv bude generována minimálně 1x měsíčně a uložena do předem domluveného adresáře pro účely nahlížení vedení úřadu a města. Dále rozhoduje o změně systémových hesel a zajišťuje zápis změn do Evidence systémových hesel. Evidence jsou vedeny z důvodu zastupitelnosti informatiků nebo oprávněných osob.

3.2 Bezpečnost přístupu třetích stran

Třetími stranami se rozumí dodavatelé IS, servisní pracovníci HW i SW, odborní konzultanti. Pro každého externího pracovníka je vytvořen zvláštní login, podle jeho funkce. Externí pracovník se do systému hlásí vždy s vědomím správce sítě. Vyžaduje-li zásah oprávnění k více než jedné aplikaci, provádí po celou dobu zásahu dohled správce sítě.

4. PERSONÁLNÍ BEZEPEČNOST

4.1 Nástup do pracovního poměru

Při nástupu do pracovního poměru je každý nový zaměstnanec seznámen se základními bezpečnostními předpisy. Zároveň s podpisem pracovní smlouvy podepíše Prohlášení o mlčenlivosti na základě zákona 101/2000 Sb. Obdrží proti podpisu klíče od kanceláře, čipovou kartu a případně podle svého zařazení i klíče od budovy. Personalista oznámí nový nástup oprávněným osobám minimálně 5 pracovních dnů předem. Přístupová práva nového zaměstnance budou nastavena dle katalogu systemizovaných pracovních míst. Změní-li se pracovní zařazení uživatele, jsou mu změněna přístupová práva podle nového systemizovaného pracovního místa. Změnu pracovního zařazení oznámí personalista oprávněným osobám minimálně 5 pracovních dnů předem.

4.2 Ukončení pracovního poměru

Při ukončení pracovního poměru uživatele je zrušen jeho účet, jeho e-mailová schránka. Data jím vytvořená v uživatelském adresáři jsou dle potřeby zpřístupněna uživateli, na kterého přechází agenda. Pracovník odevzdá všechny klíče od všech prostor, které využíval a přístupovou kartu. Obdrží protokol o vrácení uvedených věcí.

4.3 Docházkový systém

Při vstupu do objektu městského úřadu je zaměstnanec povinen přihlásit se zaměstnaneckou kartou. Při jakémkoli opuštění objektu je zaměstnanec povinen odhlásit se z docházkového systému.

4.4 Školení uživatelů

4.4.1 Bezpečnost práce

Školení o bezpečnosti práce je povinen absolvovat každý nový pracovník v době do 7 dnů po nástupu.

4.4.2 Vstupní školení

Vstupní školení pracovníků zahrnuje 2 fáze. Seznámení s legislativou ČR probíhá v rámci elearningu. V rámci školení na městském úřadu jsou zaměstnanci seznámeni s vnitřními předpisy, pracovními postupy, s informačním systémem úřadu atd.

4.4.3 Průběžná školení

Průběžná školení jsou plněna především prostřednictvím e-learningu.

4.4.4 Zvláštní odborná způsobilost

Školení ZOZ probíhá na personálním oddělení.

4.5 Odpovědnost uživatelů

Všem uživatelům informačních systémů, aplikací a sítí poskytují informatici potřebné bezpečnostní poradenství. Porušení zákona o ochraně dat a osobních údajů, zneužití informací a porušení mlčenlivosti bude posuzováno a řešeno v souladu se Zákoníkem práce a Pracovním řádem jako porušení pracovní kázně. S tímto je nový zaměstnanec seznámen při nástupu do pracovního poměru při podpisu **Prohlášení o mlčenlivosti.**

4.6 Obecná odpovědnost

Všichni zaměstnanci nebo další subjekty spadající pod úřad musí:

- Chránit HW, SW a informace, které jsou jim svěřeny
- Chránit průnik škodlivého programového vybavení do informačních systémů úřadu
- Hlásit veškerá podezření na bezpečnostní ohrožení

5. FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

5.1 Definice pracovišť

5.1.1 Serverovna a technické místnosti

Servery, switche a EZS jsou umístěny v určených místnostech. Klíče od těchto místností jsou oprávněni vlastnit pouze pověření zaměstnanci. Je-li v těchto místnostech nezbytná přítomnost třetí osoby, děje se tak jedině za přítomnosti nejméně jednoho z pověřených zaměstnanců. V každé z těchto místností je vedena evidence návštěv třetích osob.

5.1.2 Speciální pracoviště

Pojem speciální pracoviště označuje prostory, ve kterých jsou zpracovávána data obsahující údaje o zvláštních skutečnostech.

5.1.3 Běžná pracoviště

Zabezpečení objektů řeší Provozní řád objektu Městského úřadu Jáchymov

5.2 Home Office

Home Office je umožněn pracovníkovi se souhlasem tajemníka nebo starosty města. Přístup bude zajištěn VPN připojením z důvodu monitorování přístupů. Tento přístup zajistí pověření pracovníci.

5.2.1 Povinnosti zaměstnance

Po udělení přístupu je zaměstnanec povinen absolvovat školení v oblasti bezpečnosti práce v rámci home office a bezpečnosti IT. Výstupem tohoto školení je protokol o proškolení v rámci home office. Dále je zaměstnanec povinný zajistit, že jeho soukromý počítač bude opatřen antivirovým systémem a že v době využívání benefitu home office nemá k PC přístup nikdo jiný. Po ukončení činnosti uzavře dokumenty, aplikace a odhlásí se z VPN.

5.2.2 Přístupy do CzechPointu na Home Office

Z bezpečnostních důvodů není možné do aplikací, vyžadující přístupy přes certifikát (token), přistupovat z domova. Token lze využít pouze za fyzické přítomnosti pracovníka u PC.

5.3 Zabezpečení zařízení

Servery jsou zabezpečeny v uzamčených místnostech (viz 5.1.1). Telefonní ústředna je umístěna v jedné z místností pro servery a přístup k ní mají jen pověřené osoby. Je-li nutný zásah třetí osoby, provádí se vždy za přítomnosti oprávněné osoby a zápisu do evidence návštěv.

6. BEZPEČNOST PROVOZU INFORMAČNÍHO SYSTÉMU

6.1 Provozní postupy a odpovědnosti

Provozní postupy jsou pro každý informační systém specifikovány v následujících dokumentech:

- Uživatelská příručka informačního systému
- Systémová příručka informačního systému
- Provozní bezpečnostní dokumentace informačního systému

6.2 Monitoring

Oprávněné osoby ve spolupráci s externím pracovníkem IT zajišťují, že jsou monitorovány potencionální bezpečnostní slabiny všech provozních aplikací, systémů a sítí. Bezpečnostní incidenty musí být v souladu s GDPR okamžitě nahlášeny pověřenci.

6.3 Plánování a akceptace systémů

U informačních systémů je sledována míra jejich využívání, aby bylo včas možné zjistit potřebu upgradu/změny provozního prostředí informačního systému z důvodu zajištění správné funkce i při nárůstu objemu zpracovávaných dat nebo počtu uživatelů. Pro nasazování informačních systémů i jejich úprav je nezbytné stanovit akceptační kritéria a provést odpovídající testy.

Při akceptaci systému je nutné zvážit požadavky systému na výpočetní a paměťový výkon, schopnost jeho zotavování z chyb, přípravu a test rutinních provozních postupů, vliv na ostatní systémy.

6.4 Antivirová ochrana

Detekci na úrovni pracovních stanic zajišťuje antivirový systém – ESET Endpoint Antivirus. Odpovědnost za to, že pro detekci a ochranu informačních systémů, aplikací a sítí proti virům a jinému škodlivému kódu existují vhodné prostředky, nesou pověřené osoby.

6.5 Webové prohlížeče

Referenti mohou využívat pouze následující prohlížeče

- Microsoft EDGE
- Chrome

Ostatní prohlížeče nejsou pro bezchybný provoz podporovány a pověřené osoby je nebudou spravovat a zabezpečovat.

6.6 Zálohování

Je prováděno pravidelné zálohování dat takovým způsobem, aby v případě incidentu bylo možné tato data zpětně k danému datu obnovit, a to až 14 dní zpět. K záložním souborům mají přístup pouze pověřené osoby a za proces zálohování a obnovy odpovídají pověřené osoby.

6.7 Podezřelá aktivita

Podezřelou aktivitou se myslí neobvyklý provoz na síti úřadu. Například vysoký objem stažených / nahraných dat z / do internetu. Pověřená osoba následně kontaktuje dotyčného uživatele a požádá o vysvětlení, jak mohlo dojít k přenesenému objemu dat.

7. ŘÍZENÍ LOGICKÉHO PŘÍSTUPU

7.1 Požadavky na řízení přístupu

Řízení přístupu je řešeno autentizací uživatelů při vstupu do systému. Každý uživatel má své jediné a nezpochybnitelné přihlašovací jméno a heslo a po přihlášení do systému má oprávnění využívat jej podle přístupových práv, která mu byla přidělena na základě jeho pracovního zařazení.

7.2 Správa přístupu uživatelů

Správa přístupu uživatelů probíhá v Active Directory. Evidenci práv se změnami přístupů vedou pověřené osoby, kteří zajišťují přidělení přístupů. O zvýšení práv uživatele žádá vedoucí odboru tajemníka nebo starostu města. Při ukončení pracovního poměru jsou všechna práva odebrána a uživatelský login je zrušen.

7.3 Uživatelská hesla

Prvotní heslo uživatelům generuje pověřená osoba, jde minimálně o deset znaků v kombinaci písmen a čísel. Platnost hesla je nastavena na 180 dnů. Po uplynutí této doby bude uživatel vyzván ke změně hesla. Následující heslo nesmí být totožné s posledními 3 hesly.

7.4 Certifikáty a tokeny

Veškeré certifikáty jsou opatřeny pin kódem a uloženy na tokenech. Vytváření a ukládání certifikátů probíhá v souladu s nařízením eIDAS.

7.5 Povinnosti uživatelů

Každý uživatel je povinen se do systému přihlásit svým přihlašovacím jménem a heslem. Heslo je uživatel povinen držet v tajnosti. V případě, že uživatel zjistí, že jeho heslo bylo vyzrazeno, oznámí tuto skutečnost okamžitě pověřené osobě. Ta zajistí okamžitou změnu hesla.

7.6 Povinnosti pověřených osob

Bezpečnostní pravidla platící pro standardní uživatele jsou povinni dodržovat i pověřené osoby. Ty jsou navíc povinni udržet v tajnosti i všechna ostatní hesla, se kterými se seznámí v rámci své činnosti. Externí pracovníci, kteří na pracoviště docházejí pravidelně, mají vytvořený vlastní zvláštní účet s právy nutnými k požadovaným servisním zásahům. Externí pracovníci pracují vždy za přítomnosti pověřené osoby. Přístupové heslo uživatele administrátor, a jeho případnou změnu, je pověřená osoba povina zapsat, vložit do obálky a obálku zalepit. Tato obálka je poté opatřena razítkem městského úřadu znemožňujícím její otevření bez zanechání stop. Obálka je následně uložena do trezoru městského úřadu. V případě nutnosti (neočekávaná nepřítomnost, zapomenutí hesla atd.) může být obálka otevřena za splnění následujících podmínek:

- Otevření obálky se zúčastní minimálně 2 osoby, z nichž alespoň jedna osoba je starosta, místostarosta nebo tajemník městského úřadu.
- Po otevření obálky se provede zápis do dokumentu Evidence poruch a mimořádných událostí informačního systému.
- Odpovědná osoba okamžitě po otevření heslo uvedené v obálce v informačním systému změní podle výše uvedených pravidel.

7.7 Vzdálený přístup

Externisté mohou využít vzdáleného přístupu, a to prostřednictvím VPN (ZyWALL, Fortinet client) vždy pod dohledem.

7.7.1 VPN

Vzdálený přístup do jednotlivých aplikací nebo částí systému může být umožněn i externím pracovníkům. Tento přístup musí být realizován VPN klientem a zabezpečený heslem. Přístup je standardně blokován, odblokování provede pověřená osoba pouze na dobu zásahu.

7.8 Řízení přístupu k operačnímu systému pracovních stanic

Každému zaměstnanci je v prostředí OS Windows vytvořen doménový účet s uživatelskými právy. Vedení města, úřadu a vedoucí pracovníci mají vytvořené doménové účty s právy lokálního administrátora účty. Na stanicích nejsou zřízeny anonymní účty nebo účty bez hesla.

7.9 Zastupitelnost uživatelů

Běžný uživatel musí dokumenty, které by mohly být ostatními zaměstnanci odboru využívány, uložit na odborový síťový disk tak, aby byly v době jeho nepřítomnosti dostupné. Pokud dojde k situaci, kdy bude nutné přečíst data, uložená na lokálním disku nepřítomného uživatele, bude přístup s vědomím jeho nadřízeného zajištěn pověřenou osobou a současně za přítomnosti alespoň jednoho zaměstnance daného odboru, nejlépe vedoucího či jeho zástupce. Data budou zkopírována na síťový disk dotčeného odboru. Pro zastupujícího pracovníka je přístup do aplikací řešen vytvořením dalšího přístupového jména a hesla pro zástupce. Je zakázáno řešit zastupitelnost sdělením přístupového hesla.

8. BEZPEČNOSTNÍ INCIDENT, ŘEŠENÍ INCIDENTU A HAVÁRIE

8.1 Bezpečnostní incident

Při řešení bezpečnostních incidentů nezpůsobených lidským faktorem (vyšší mocí, technickou havárií apod.) je kladen důraz především na rychlé obnovení normálního provozu. Obnova techniky může být zajištěna zápůjčkou, obnova dat se provede ze zálohy. Po zajištění provozu budou přijata opatření k zabránění opakování incidentu. Řešení bezpečnostních incidentů způsobených nedbalostí nebo úmyslně odpovědnou osobou spočívá jednak v rychlém obnovení provozu a jednak v analýze incidentu a vyvození důsledku (porušení pracovní kázně).

8.2 Řešení incidentů

8.2.1 Identifikace incidentu

Incident je ihned po jeho zjištění nahlášen telefonicky a následně potvrzen v písemné formě emailem vedoucímu příslušného odboru, tajemníkovi a starostovi města.

8.2.2 Oznámení incidentu

Bezpečnostní incident v rámci IS MěÚ je neprodleně řešen informatiky a podle charakteru incidentu také v součinnosti s pověřencem GDPR.

8.2.3 Analýza incidentu.

Pověřené osoby provedou zjištění přesného rozsahu, a pokud je to možné i příčiny incidentu.

8.2.4 Oznámení bezpečnostního incidentu

Po analýze rozsahu, příčin a možných důsledků jsou na bezpečnostní událost emailem a následně telefonicky upozorněni všichni nebo dotčení uživatelé IS, a současně je jim sdělen rozsah dočasných omezení provozu informačního systému (pokud k nim v důsledku incidentu dojde).

8.2.5 Nouzový režim provozu IS

Je-li to relevantní a vyžaduje-li to konkrétní situace (zejména potrvá-li odstranění následků incidentu delší dobu), stanoví pověřené osoby ve spolupráci s tajemníkem, starostou města (v případě potřeby také s vedoucími dotčených odborů), náhradní nouzový režim provozu IS. Pověřené osoby vydají potřebné pokyny pro nouzový režim provozu IS platné až do jeho odvolání.

8.2.6 Následky incidentu jsou odstraněny

Celý průběh včetně řešení je zaevidován. Pokud byl stanoven nouzový režim provozu IS, je tento po otestování správné funkčnosti IS odvolán. Záznamy o vzniku, průběhu, důsledcích a řešení bezpečnostní události musí být uloženy u pověřených osob chráněny proti neautorizované manipulaci.

8.2.7 Vyhodnocení incidentu a přijetí opatření

Podle charakteru incidentu jsou vyvozeny důsledky. Jedná se například o vznik nového požadavku na IS města, který zabrání opakování stejné, změnu či doplnění interních směrnic města, poučení uživatelů, proč k incidentu došlo apod. V případě ohrožení důvěrnosti dat v IS je v obecném smyslu postupováno podle platné legislativy ČR, této Bezpečnostní politiky a dalších relevantních interních směrnic města.

8.3 Havárie

Dojde-li k havárii nebo hrozí-li havárie ohrožující majetek nebo bezpečnost osob celého úřadu, její likvidace je řešena v souladu s Evakuačním plánem MěÚ. Za řešení havárie IS odpovídají pověřené osoby. Jedná-li se o havárii systému, na který je sjednána smluvní podpora, spolupracuje s pověřenými

osobami dodavatel. Pokud dojde k porušení nařízení GDPR, musí se taková skutečnost ihned nahlásit pověřenci.

9. HODNOCENÍ RIZIK

9.1 Audit

Pověřené osoby provádějí namátkové kontroly bezpečnostních rizik u všech procesů, které jsou pokryty touto bezpečnostní politikou. Kontroly rizik se týkají všech informačních systémů, aplikací, sítí i uživatelů. Audit probíhá pomocí konzole ESET.

9.1.1 Audit SW

Pověřené osoby provádějí namátkové audity nainstalovaného softwaru a ručí za to, že veškerý nainstalovaný software je legální. Audit probíhá pomocí konzole ESET. V případě porušení nastavených pravidel budou zaměstnanci postihováni dle kapitoly 9.3.

9.2 Způsob hodnocení rizik

Hodnocení rizik probíhá průběžně, a to v souladu s touto bezpečnostní politikou.

9.3 Sankce za porušení Bezpečnostní politiky

Jakékoli porušení povinností vyplývajících z Bezpečnostní politiky bude posuzováno jako porušení pracovních povinností, porušení Pracovního řádu a bude postihováno podle zákona 262/2006 Sb., zákoník práce v platném znění, § 52, odstavec g) s následkem snížení, případně odebrání osobního příplatku až výpověď z pracovního poměru.

10. LEGISLATIVNÍ POŽADAVKY

10.1 Soulad s právními normami

Dokument Bezpečnostní politika MěÚ Jáchymov je vypracován tak, aby plně odpovídal požadavkům uvedeným v následujících právních předpisech:

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (zákon o ISVS).
- Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy).
- Vyhláška č. 53/2007 Sb., o technických a funkčních náležitostech uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictvím referenčního rozhraní (vyhláška o referenčním rozhraní).
- Zákoník práce 262/2006 Sb., ve znění pozdějších předpisů
- Zákon č. 128/2000 Sb., o obcích, v platném znění
- Zákon č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů
- Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů
- Vyhláška č. 512/2002 Sb., o zvláštní odborné způsobilosti úředníků územních samosprávných celků
- Zákon o účetnictví (563/1991 Sb.)
- Zákon o archivnictví a spisové službě a o změně některých zákonů (499/2004 Sb.)
- Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon – 121/2000 Sb.)
- Zákon o krizovém řízení a o změně některých zákonů (krizový zákon – 240/2000 Sb.)

- Zákon č. 297/2016Sb., zákon o službách vytvářejících důvěru pro elektronické transakce
- Zákon o svobodném přístupu k informacím (106/1999 Sb.)
- Nařízení (EU) 2016/679 (GDPR)

10.2 Navazující dokumenty

Dokumenty navazujícími na tuto bezpečnostní politiku jsou: Organizační řád, Skartační řád, Pracovní řád

Mgr. et Mgr. Michal Baláž, DiS.
Starosta města