Úřad městské části Praha 5

Informační koncepce ISVS

Projekt:	Atestace IS Úřadu městské části Praha 5 dle Zákona č. 365/2000 Sb. o informačních systémech veřejné správy a vyhlášky č. 529/2006 Sb. o dlouhodobém řízení ISVS
Předmět:	Provozní bezpečnostní dokumentace – systémová bezpečnostní příručka

Vlastník dokumentu: MČ Praha 5 Nám. 14. října č. 4 15022 Praha 5	Aktualizace dokumentu:: PERGO s.r.o. V Jámě 699/1 Praha 1, 110 00

Revize dokumentu

Poř. číslo:	Datum	Revize:	Revizi provedl	Výsledek revize schválil/dne
1.	25. 09. 2017	Aktualizace pojmů	P. Šimko	18. 10. 2018 P. Šimko
2.	30. 09. 2017	Aktualizace údajů	Bc. Tesařová	18. 10. 2018 P. Šimko
3.	16. 11. 2017	Revize pojmů	PERGO s.r.o.	16. 11. 2018 P. Šimko/ Bc. Tesařová
4.	18. 5. 2018	Celková aktualizace	PERGO s.r.o.	21. 5. 2018 P. Šimko/ Bc. Tesařová

Platnost dokumentu

Ověřil:	Mgr. Viglaský, MPA	Dne		Podpis:
Schválil:	Bc. Žebera	Dne		Podpis:
Účinnost od:	1. 6. 2018			
Vydal:	ÚMČ Praha 5			
Počet stran:	27			
Počet příloh:	1			
Vydání:	verze 4.0			
dokument	**INTERNÍ**			

OBSAH:

1. Úvod

Informační koncepce je dokument, v němž Úřad městské části Praha 5 stanovuje své dlouhodobé cíle v oblasti dlouhodobého řízení IS.

Jsou v něm definovány cíle v oblasti bezpečnosti a kvality spravovaných ISVS. Rovněž jsou stanovena základní pravidla pro pořizování a provozování ISVS.

1.1. Základní údaje o organizaci

V následující tabulce jsou uvedeny základní identifikační údaje Úřadu městské části Praha 5.

Název organizace:	Úřad městské části Praha 5
IČ:	000 63 631
Adresa:	nám. 14. října č. 4, 150 22 Praha 5
Telefon:	234 378 111, 800 800 005
E-mail:	podatelna@praha5.cz
Web:	www.praha5.cz
Kontaktní osoba pro oblast ICT:	Bc. Petra Tesařová, vedoucí odboru informatiky

Aktualizace dokumentu:

Název organizace:	PERGO s.r.o.
IČ:	261 69 746
Adresa:	V Jámě 699/1
Telefon:	+420 603 862 081, +420 608 614 277
E-mail:	info@pergosro.cz
Web:	www.pergosro.cz
Kontaktní osoba:	Bc. Jiří Čelikovský, konzultant

1.2. Základní údaje o Informační koncepci

Název dokumentu:	Informační koncepce Úřadu městské části Praha 5
Datum schválení aktuální verze:	1. 6. 2018

Způsob schválení:	Vzato na vědomí dne ..... Radou MČ Praha 5 (číslo usnesení .....)
Doba platnosti:	5 let/pravidelná roční revize
Umístění dokumentu:	Intranet úřadu – Vnitřní organizační předpisy https://intranet.praha5.cz/
Aktuální verze:	4.0

1.3. Údaje o předchozích verzích

V této kapitole jsou uvedeny všechny změny provedené v dokumentu, tak jak byly po jeho schválení postupem času prováděny.

Změny dokumentu jsou prováděny především po provedení zásadních změn v Informačním systému Úřadu městské části Praha 5 (dále jen IS ÚMČ) nebo po provedení pravidelného vyhodnocení dodržování Informační koncepce.

Verze 4.0 je vydána s účinností od 1. 6. 2018. První atestace ISVS provedena na základě tohoto dokumentu byla vydána s platností od 4. 12. 2009. Aktualizace proběhla na základě výstupů z kontroly provedené v první polovině roku 2018 Ministerstvem vnitra.

2. Zdroje a východiska

2.1. Přehled zdrojů použitých pro tvorbu Informační koncepce

Zdroji z městské části použitých pro tvorbu Informační koncepce jsou jak dokumenty strategické, tak dokumenty zaznamenávající stav IS k danému datu a další záměry:

- Programové prohlášení Zastupitelstva MČ Praha 5
- Program rozvoje městské části Praha 5
- Směrnice č. 8/2013 Standardy informačního a komunikačního systému ÚMČ
- ČSN ISO/IEC 27001 a ISO 9001
- Směrnice č. 10/2017 O provozu budov Úřadu
- Organizační řád ÚMČ Praha 5 – 2018
- Dokumentace Integrovaného systému řízení ÚMČ Prahy 5, zejména:
    - Bezpečnostní management – manažeři bezpečnosti oblastí procesů a aktivit dle QMS a ISMS
    - Uživatelská příručka ISMS
    - Příručka QMS a ISMS, a další.

Inspirativním a významným faktorem při budování a rozvíjení informačního systému jsou pravidelné schůzky Magistrátu hl. města Prahy a úřadů jednotlivých městských částí, jejichž hlavním cílem je vzájemná spolupráce, řešení důležitých otázek v oblasti informatiky a předávání informací.

Vzhledem k členství ČR v EU, je nutné brát v úvahu i strategické dokumenty EU týkající se informačních technologií.

Informační koncepce musí zohledňovat informační strategie, globální strategie či jiné podobné strategické dokumenty jak vyšších organizačních celků, tak úřadu samotného.

Za stěžejní dokumenty a projekty v celostátním měřítku pak lze považovat tyto:

- Státní informační a komunikační politika,
- Koncepce budování informačních systémů veřejné správy,
- Akční plán realizace státní informační politiky,
- Program informatizace územních orgánů veřejné správy,
- Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice č. 95/46/ES (Obecné nařízení o ochraně osobních údajů).

2.2. Legislativní rámec

Ze základní legislativy ČR v oblasti informatiky je pro provozování ISVS nejvýznamnější zákon č. 365/2000 Sb., o informačních systémech veřejné správy ve znění pozdějších předpisů. Zákon byl novelizován následujícími právními úpravami:

- č. 517/2002 Sb.,
- č. 444/2005 Sb.,

- č. 81/2006 Sb.

Pro provozování ISVS jsou důležité i následující předpisy a vyhlášky:

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění zákona č. 517/2002 Sb. a vyhlášky č. 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy,
- Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů,
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,
- Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek,
- Zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek,
- Vyhláška č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti),
- Vyhláška č. 53/2007 Sb., o referenčním rozhraní,
- Vyhláška č. 52/2007 Sb., o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb ISVS prostřednictvím referenčního rozhraní,
- Vyhláška č. 530/2006 Sb., o postupech atestačních středisek při posuzování dlouhodobého řízení ISVS,
- Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy,
- Vyhláška č. 528/2006 Sb., o informačním systému o informačních systémech veřejné správy
- Vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Vyhláška 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
- Vyhláška 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Vyhláška 437/2017 Sb., o kritériích pro určení provozovatele základní služby
- Zákon č. 131/2000 Sb., zákon o hlavním městě Praze
- NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 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)

3. Přehled provozovaných ISVS a provozních agend s vazbou na ISVS

Pro účely Informační koncepce byl sestaven seznam všech informačních systémů a agend používaných v rámci úřadu. Kompletní seznam je přílohou této Informační koncepce.

Pro účel Informační koncepce pak byly ze seznamu vybrány agendy a informační systémy, které splňují definici ISVS a dle platné legislativy tedy podléhají procesu dlouhodobého řízení ISVS.

V dokumentu jsou popsány ISVS a provozní systémy splňující následující podmínky:

- úřad je správcem ISVS
- provozní agenda má vazbu na jiný ISVS

V dokumentu tedy nejsou popsány provozní systémy, které nemají žádnou vazbu na jakýkoliv ISVS.

Každý provozovaný ISVS je pak popsán za pomoci následujících atributů:

- úplný název agendy,
- zkratka názvu agendy,
- související právní předpisy,
- útvar zajišťující provoz ISVS,
- charakteristika ISVS,
- zpracovávaná data,
- technické a programové prostředí,
- současný stav ISVS,
- předpokládané změny

Každá provozní agenda s vazbou na ISVS je popsána následujícími atributy:

- úplný název agendy,
- zkratka názvu agendy,
- související právní předpisy,
- útvar zajišťující provoz agendy,
- charakteristika agendy,
- současný stav agendy,
- popis vazby na ISVS

3.1. Informační systémy veřejné správy

3.1.1 Elektronická podatelna

Úplný název ISVS:	Elektronická podatelna (modul GINIS SSL)
Zkratka názvu:	EPOD
Právní předpisy:	Nař. vlády ČR č. 304/2001, zák. č. 227/2000 Sb.
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Aplikace zajišťující provoz elektronické podatelny za pomoci kvalifikovaných certifikátů
Zpracovávaná data:	Údaje o podáních
Technické a programové prostředí:	Windows 2013 Server, Windows 10 na klientských stanicích
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS jsou plánovány změny spočívající v digitalizaci analogových dokumentů.

3.1.2 GINIS SSL

Úplný název ISVS:	GINIS spisová služba
Zkratka názvu:	SSL
Právní předpisy:	Zákon 499/2004 Sb. o archivnictví a spisové službě, ve znění pozdějších předpisů
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Komplexní vedení spisové služby. Automatizuje evidenci a oběh písemností v celém jejich životním cyklu.
Zpracovávaná data:	Údaje o písemnostech
Technické a programové prostředí:	Windows 2013 Server, Windows 10 na klientských stanicích
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.3 PROXIO Agendio – Evidence soudních sporů

Úplný název ISVS:	PROXIO Agendio – Evidence soudních sporů
Zkratka názvu:	
Právní předpisy:	
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Komplexní vedení agendy evidence soudních sporů. Automatizuje evidenci a oběh písemností týkajících se soudních sporů v celém jejich životním cyklu.
Zpracovávaná data:	Údaje o soudních sporech a vymáhání pohledávek na Odboru legislativním
Technické a programové prostředí:	Windows 2013 Server, Windows 10 na klientských stanicích na klientských stanicích
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.4 PROXIO Agendio – Usnesení, zápisy, úkoly

Úplný název ISVS:	PROXIO Agendio – Usnesení, zápisy, úkoly
Zkratka názvu:	
Právní předpisy:	Zákon 131/2000 Sb. o hlavním městě Praze
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Komplexní workflow pro materiály jednotlivých orgánů MČ Praha 5 včetně jejich archivace a zveřejnění na portálu MČ Praha5
Zpracovávaná data:	Zpracování materiálů pro jednání RMČ, ZMČ, komisí a výborů MČ Praha 5
Technické a programové prostředí:	Windows 2013 Server, Windows 10 na klientských stanicích
Současný stav:	ISVS je v testovacím provozu.
Předpokládané změny:	Pro tento ISVS je po uvedení do rutinního provozu plánována integrace na hlasovací systém zasedání ZMČ

3.2. Provozní agendy s vazbou na ISVS

3.2.1 GINIS EKO

Úplný název ISVS:	GINIS EKO
Zkratka názvu:	EKO
Právní předpisy:	Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Ekonomické agendy GINIS
Vazba na ISVS:	Předávání účetních výkazů na MHMP

3.2.2 Datacentrum 2

Úplný název ISVS:	Datacentrum 2
Zkratka názvu:	DC2
Právní předpisy:	Nařízení vlády 564/2006 Sb., zákon 262/2006 Sb.
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Personální a mzdová agenda
Vazba na ISVS:	Systém komunikuje s PSSZ, Finančním úřadem a poskytuje data do Informačního systému o platech dle předepsané datové struktury.

3.2.3 R-Info

Úplný název ISVS:	R-Info
Zkratka názvu:	R-Info
Právní předpisy:	Nařízení vlády 564/2006 Sb., zákon 262/2006 Sb.
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Evidence místních a správních poplatků, výherní automaty
Vazba na ISVS:	Systém vytváří a spravuje data o poplatcích, které vznikají v místní příslušnosti MČ Praha 5.

3.2.4 EVI 8

Úplný název ISVS:	Evidence odpadů
Zkratka názvu:	EVI 8
Právní předpisy:	Zákon o odpadech č. 185/2001 Sb., vyhlášek č. 381/2001 Sb., 383/2001 Sb., přílohy č. 19, 20, 22, 23, 24, 26, 27, č. 352/2005 Sb., přílohy č. 8, č. 352/2008 Sb., přílohy č. 3, 4 a 5.
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	IS zajišťuje služby evidence odpadů.
Vazba na ISVS:	IS pokrývající evidenci odpadů při každém vzniku, zneškodnění nebo předání odpadu, hlášení o produkci a nakládání s odpady, výkaz ODP 5-01 pro Český statistický úřad.

3.2.5 PROXIO Agendio – Evidence obyvatel (Ohlašovna)

Úplný název ISVS:	PROXIO Agendio – Evidence obyvatel (Ohlašovna)
Zkratka názvu:	
Právní předpisy:	Zákon 133/2000 Sb. o evidenci obyvatel
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Komplexní podporu pro zajištění činností spojených se zpracováním údajů registru obyvatel MČ Praha5
Zpracovávaná data:	Data o občanech MČ Praha 5 včetně provádění změn v ROB (přistěhování, odstěhování, změna)
Technické a programové prostředí:	Windows 2013 Server, Windows 10 na klientských stanicích
Současný stav:	ISVS je v rutinním provozu.
Vazba na ISVS:	Vazba na ISZR

3.2.6 PROXIO Agendio – Volební agenda

Úplný název ISVS:	PROXIO Agendio – Volební agenda
Zkratka názvu:	
Právní předpisy:	• Zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů • Zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů a o změně některých zákonů • Zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů • Zákon č. 62/2003 Sb., o volbách do Evropského parlamentu a o změně některých zákonů • Ústavní zákon č. 71/2012 Sb., o zavedení přímé volby prezidenta • Zákon č. 22/2004 Sb., o místním referendu a o změně některých zákonů • Prováděcí vyhlášky výše zmíněných zákonů • Metodika k distribuci, evidenci, skladování a k dalším pravidlům zacházení s voličským průkazem od 1. 1. 2014 • Metodika k vedení seznamu voličů pro volby do Evropského parlamentu konané v roce 2014 • Metodika k novým postupům při vedení seznamu voličů a volebních okrsků od 1. ledna 2014 Zákon 133/2000 Sb. o evidenci obyvatel
Provoz zajišťuje:	Odbor informatiky
Charakteristika:	Komplexní podporu pro zajištění činností spojených s organizací a průběhem parlamentních, komunálních a prezidentských voleb na území MČ Praha5
Zpracovávaná data:	Data o občanech MČ Praha 5, volebních komisích, volebních okrscích a politických stranách.
Technické a programové prostředí:	Windows 2013 Server, Windows 10 na klientských stanicích
Současný stav:	ISVS je v rutinním provozu.
Vazba na ISVS:	Vazba na ISZR

4. Záměry na pořízení nových ISVS

Pokud bude Úřad městské části Praha 5 pořizovat nebo budovat nový ISVS, pak je třeba dodržet následující zásady.

4.1. Zásady při pořizování nových ISVS

Vlastnímu pořízení nového ISVS předchází v podmínkách Úřadu MČ Praha 5 nejprve formulace záměru na pořízení nového ISVS.

Záměr na pořízení ISVS je materiál v písemné nebo elektronické formě, který obsahuje základní fakta o novém ISVS včetně důvodu k jeho pořízení.

Záměr na pořízení ISVS obsahuje následující údaje:

- název ISVS,
- související právní předpisy
- důvod pořízení,
- zpracovávaná data a poskytované služby,
- útvar zajišťující provoz ISVS,
- náklady na pořízení a provozní náklady,
- požadavky na lidské zdroje,
- termín realizace a termín spuštění rutinního provozu.

Záměr na pořízení ISVS je vypracován vnitřním útvarem úřadu (odbor, oddělení) obvykle na základě požadavku vedoucího odboru, tajemníka úřadu, člena Zastupitelstva MČ, popř. zřízeného fóra či výboru.

O akceptaci či odmítnutí záměru rozhoduje pracovní skupina složená z:

- pracovníka oddělení informatiky,
- pracovník správy sítě,
- vedoucího Odboru informatiky,
- tajemníka úřadu.

Složení pracovní skupiny se může operativně měnit v závislosti na typu navrhovaného ISVS.

Pokud pracovní skupina doporučí záměr realizovat, je nadále pořízení nového ISVS řešeno jako samostatný projekt.

Celý systém řízení projektu má definovanou strukturu a je závazný pro všechny subjekty, které se na projektu podílejí během celého životního cyklu projektu.

5. Řízení kvality ISVS

Informační systém Úřadu MČ Praha 5 je systém dosti rozsáhlý – přistupuje k němu cca 380 uživatelů. Správa informačního systému takového rozsahu klade nároky nejen na hardware a sítě, ale celkem logicky i na systém jeho dlouhodobého řízení.

5.1. Stanovení dlouhodobých cílů kvality ISVS

Z výše uvedených důvodů probíhá budování IS ÚMČ jako informačního systému který bude:

- splňovat platnou legislativu ČR/EU,
- naplňování cílů E-Governmentu,
- umožňovat rychlejší dosahování cílů úřadu ve všech oblastech,
- budován s důrazem na transparentnost – veškeré postupy jsou dokumentovány,
- uživatelům důvěryhodným zdrojem aktuálních a ověřených informací s vysokou mírou použitelnosti a vysokou užitnou hodnotou – kvalita služeb,
- bezpečný a spolehlivý.

Jednotlivé cíle kvality řízení a bezpečnosti informací jsou vedeny v samostatném, průběžně aktualizovaném, dokumentu. Záznam o cíli viz tabulka níže. V případě, že cíl bude přímo dopadat na kvalitu zpracovávaných dat, zajišťovaných služeb či kvalitu technických a programových prostředků, bude tato skutečnost popsána u specifikace cíle.

Poř. č.	Cíl	Zdroje	Odpovědný	Termíny	Kontrolu je	Výstup Ukončení
1	**Kvalita zpracovávaných dat - Zvýšení integrity dat –** zajištění kontrolních mechanismů pro kontrolu zadávaných údajů, pravidelná údržba databází	Provozní	OIN	Průběžně	Interní audit, kontrolní dny OIN	Záznam v přezkoumání systému, kvalitní, celistvá data
2	**Kvalita zpracovávaných dat –** Údaje v evidencích a IS jsou zpracovávány v souladu s obecně závaznými předpisy – zajištění souladu s požadavky zákonů 111/2009 Sb., o základních registrech, 101/2000 Sb., o OOÚ a GDRP	Provozní	OIN	Průběžně	Interní audit	Záznam v přezkoumání systému, data zpracovávaná v souladu s legislativou
3	**Kvalita zajišťovaných služeb –** Dostupnost služeb IS – zajištění vysoké dostupnosti služeb IS	Provozní	OIN	Průběžně	Interní audit, kontrolní dny OIN	Vysoká dostupnost služeb
4	**Kvalita zajišťovaných služeb – HelpDesk –** Zabezpečení kvalitního vyřizování requestů uživatelů a jejich reporting	Provozní	OIN	Průběžně	Kontrolní dny OIN, interní audit	Kvalitně a včas vyřízené požadavky uživatelů IS
5	**Kvalita technických a programových prostředků –** Provozní výkon a stabilita – Zajištění stabilního provozu IS a technických prostředků, Pravidelná obměna technologií, pravidelné aktualizace softwarových prostředků	Provozní	OIN	Průběžně	Kontrolní dny OIN, interní audit	Provoz s minimem poruch a výpadků

6	**Kvalita technických a programových prostředků –** povinná provozní dokumentace ISVS dle zákona	Provozní	OIN	Průběžně	Interní audit	Soulad s platnou legislativou

5.2. Role a odpovědnosti v oblasti řízení kvality

Při budování IS ÚMČ je důsledně uplatňován projektový způsob řízení. Totéž platí i v oblasti zajištění kvality. Každá změna, popřípadě pořízení nové části informačního systému (agenda, inf. systém, technické řešení,…) v IS ÚMČ je vždy řešena jako samostatný projekt.

Jednotlivé role při budováni IS ÚMČ (a zároveň v systému zajištění kvality) jsou delegovány na jednotlivé organizační složky úřadu v závislosti na povaze konkrétního projektu.

Celý systém řízení projektu má definovanou strukturu a je závazný pro všechny subjekty, které se na projektu podílejí během celého životního cyklu projektu.

Ve vztahu k řízení systému jakosti jsou to zejména následující:

Vedoucí projektu

- odpovídá za průběh projektu a řídí projektový tým,
- je zodpovědný za výběr dodavatelů a případných externích spolupracovníků
- mimo jiné je i zodpovědný za dosahování cílů v oblasti zajištění kvality.

Projektový tým

- je zodpovědný za realizaci zadání v oblasti zajištění kvality během celého životního cyklu projektu,
- zajišťuje kompletně řešení projektu spolu s případnými externími dodavateli a spolupracovníky,
- podléhá vedoucímu projektu.

Garant projektu

- je nejvyšším orgánem řízení projektu a vrcholným rozhodovacím orgánem,
- rozhoduje zejména o strategicky významných okolnostech,
- pravidelně sleduje a kontroluje průběh dosahování cílů v oblasti zajištění kvality,
- je koordinátorem projektu a jeho vazeb na okolí,
- určuje konkrétní termíny v průběhu projektu,
- je zodpovědný za celkovou koncepci a architekturu řešení konkrétního projektu.

V podmínkách Úřadu MČ Praha 5 se obvykle jedná o vedoucího odboru, popř. tajemníka úřadu.

5.3. Způsob plnění požadavků na kvalitu ISVS

Nedílnou součástí zadání každého projektu (pořízení nebo změna stávajícího ISVS) je stanovení požadavků na kvalitu. Provádí se vždy konkretizací všech základních cílů řízení kvality a jejich povaha je vždy závislá na povaze konkrétního projektu.

Typickými požadavky na kvalitu jsou například:

- včasná aktualizace údajů,
- identifikace autorů dat,
- stanovení metodiky testování ISVS,
- organizační směrnice provozu ISVS,
- rozsah dokumentace implementace a provozu ISVS.

Za stanovení dílčích požadavků je zodpovědný garant projektu, popřípadě vedoucí projektu.

Implementaci požadavků na kvalitu pak provádí projektový tým v závislosti na termínech řešení a s ohledem na postupu řešení jednotlivých úloh.

5.4. Vyhodnocování řízení kvality

Vyhodnocování řízení kvality provádí garant projektu spolu s vedoucím projektu. Vyhodnocování kvality je součástí obvyklých kontrolních činností při řízení každého projektu. Součástí tohoto procesu je dokumentace systému řízení kvality, která je součástí projektové dokumentace.

Jedná se obvykle o následující dokumenty:

- zápisy ze schůzí organizačních složek projektu,
- průběžné zprávy o stavu projektu,
- zprávy o výsledcích testování.

5.5. Řízení kvality při rutinním provozu ISVS

Při běžném provozu ISVS pracovník odpovědný za řízení kvality provádí pravidelné kontroly dosahování cílů řízení kvality a plnění konkrétních požadavků na kvalitu. Proces vyhodnocování pak provádí pracovník odpovědný za řízení kvality ve spolupráci se správci (administrátory) jednotlivých ISVS.

Pracovník odpovědný za řízení kvality udržuje seznam požadavků na kvalitu, které byly stanoveny při pořízení každého ISVS. Ze seznamu jsou vyřazeny požadavky na kvalitu, které nejsou při běžném provozu relevantní (měly význam pouze ve fázích pořízení či implementace daného ISVS). Zbylé požadavky pak podléhají pravidelnému vyhodnocování.

Vyhodnocování probíhá minimálně 1x ročně v rámci přezkoumání systému vedením.

6. Řízení bezpečnosti ISVS

Strategickým dokumentem v oblasti řízení bezpečnosti je Bezpečnostní politika informačního systému Úřadu MČ Praha 5. Je souhrnem bezpečnostních předpisů a zásad definujících způsob zabezpečení provozu provozovaných ISVS.

Pomocí bezpečnostní politiky jsou stanovena *základní pravidla* zajišťující bezpečný provoz, integritu uložených dat a řízení přístupů k datům pro oprávněné uživatele na základě jejich funkčního zařazení v organizační struktuře organizace.

Bezpečnostní politika *určuje normy, pravidla a předpisy*, které definují způsob správy, ochrany a distribuce citlivých informací a jiných konkrétních informačních zdrojů v rámci úřadu. Specifikuje bezpečnostní opatření a způsob jejich implementace, určuje způsob použití, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky úřadu.

Bezpečnostní politika IS ÚMČ rovněž obecně *definuje bezpečné používání* informačních zdrojů.

6.1. Stanovení dlouhodobých cílů v oblasti bezpečnosti

SMART přístup

Hlavním vytyčeným cílem Úřadu je zachování dostupnosti, důvěrnosti a integrity informací spojených s výkonem státní správy, informací smluvních třetích stran, osobních údajů svých zaměstnanců a občanů (v definovaném a schváleném rozsahu – viz Příručka ISMS).

Vzhledem k tomu, že se Úřad rozhodl při definování cílů postupovat v souladu s pravidly SMART, je výše uvedený cíl dále rozpracován do konkrétních menších cílů, které byly definovány na základě výsledků provedené analýzy rizik a respektují pravidla SMART:

- S – Specific – Cíl musí být srozumitelně a jasně popsán
- M – Measurable – To, zda bylo dosaženo vytyčeného cíle, musí být měřitelné a kontrolovatelné
- A – Aligned – Cíl musí plně odpovídat potřebám člověka, pro kterého je určen
- R – Realistic – Dosažení cíle musí být reálné
- T – Timed – Musí být stanovena doba, do kdy je potřeba vytyčeného cíle dosáhnout

Jednotlivé cíle kvality řízení a bezpečnosti informací jsou vedeny v samostatném, průběžně aktualizovaném, dokumentu. Záznam o cíli viz tabulka níže. V případě, že cíl bude přímo dopadat na bezpečnosti dat, služeb, technických či programových prostředků, bude tato skutečnost popsána u specifikace cíle.

Poř. č.	Cíl	Zdroje	Odpovědný	Termíny	Kontroluje	Výstup Ukončení
1.	**Bezpečnost dat, služeb, technických a programových prostředků –** Evidence aktiv – vytvoření a údržba seznamu informačních aktiv a určení odpovědnosti	80 000 Kč	OIN/KMČ	31. 12. 2018, dále průběžně	Interní audit	Soupis aktiv s vlastníky a ohodnocením
2	**Bezpečnost dat, služeb, technických a programových prostředků –** Bezpečnost lidských zdrojů – Zajištění vysokého bezpečnostního povědomí uživatelů	30 000 Kč	KMČ	Průběžně	Interní audit	Zvýšení bezpečnosti, proškolený personál

3	**Bezpečnost dat, služeb, technických a programových prostředků –** řízení přístupu – řízení přístupu uživatelů k IS a službám	Provozní	OIN	Průběžně	Kontrolní dny OIN, Interní audit	Zvýšení bezpečnosti, snížení rizika ztráty či poškození dat
4	**Bezpečnost dat, služeb, technických a programových prostředků – Fyzické zabezpečení – předcházení neautorizovanému přístupu k aktivům**	Provozní/ projektové	KMČ/OIN	Průběžně	Interní audit, Kontrolní dny OIN	Zvýšení bezpečnosti, snížení rizika ztráty či poškození aktiv
5	**Bezpečnost dat, služeb, technických a programových prostředků –** Ochrana koncových stanic – opatření proti malwaru	Provozní	OIN	Průběžně	Kontrolní dny OIN	Zvýšení bezpečnosti, snížení rizika odcizení dat
6	**Bezpečnost dat, služeb, technických a programových prostředků** – Zálohování – opatření proti ztrátě dat	Provozní	OIN	Průběžně	Kontrolní dny OIN	Zvýšení bezpečnosti dat
7	**Bezpečnost dat, služeb, technických a programových prostředků** – Bezpečnostní požadavky na dodavatele – Stanovení bezpečnostních požadavků s dodavateli služeb, kteří mají přístup k aktivům	Provozní	OIN	Průběžně/ při uzavírání smlouvy	Interní audit	Bezpečná spolupráce, jasně dané odpovědnosti

6.2. Základní požadavky na bezpečnost

Požadavky na bezpečnost ISVS jsou konkretizací bezpečnostních cílů:

TRVALÉ A KVALITNÍ ZAJIŠTĚNÍ DOSTUPNOSTI, DŮVĚRNOSTI, INTEGRITY A AUTENTIZACE DAT

- zajištění soukromí uživatelů – ochrana uživatele před zjištěním nebo zneužitím jeho identity jinými uživateli nebo cizími osobami,
- identifikace a autentifikace uživatelů – zajištění přístupu k datům (prohlížení, aktualizace) IS ÚMČ pouze pro oprávněné uživatele a to na základě jejich funkčního zařazení,
- řízení provozu a monitoring počítačové sítě,
- existence systému pravidelného zálohování a archivace dat,
- existence plánu obnovy provozu IS (nebo jeho kritických částí) po havárii,

OCHRANA DAT A PROSTŘEDKŮ IS

- zajištění personální bezpečnosti,
- zajištění fyzické bezpečnosti prostředků IS ÚMČ,
- existence systému komplexní ochrany před škodlivými programy (viry, nepřátelské kódy),
- vybudování bezpečnostních mechanismů vůči napadení zevnitř (bezpečnostní pravidla, jak se mají uživatelé chovat),

- ochrana IS ÚMČ před napadením z externích sítí – bezpečnostní opatření zamezující možnosti průniku do vnitřní sítě (ochrana serverů, aktivních prvků a uživatelských stanic),

- ustanovení správce agendy (ISVS nebo provozní agendy).

ZAJIŠTĚNÍ BEZPEČNÉ KOMUNIKACE S OKOLÍM

- bezpečná komunikace mezi úřadem a jinými subjekty (především s orgány veřejné správy),

- používání bezpečných komunikačních cest,

- používání prostředků pro šifrování přenášených dat.

6.3. Role a odpovědnosti v oblasti řízení bezpečnosti

Bezpečnost IS ÚMČ spadá do oblasti provozní problematiky úřadu, proto *schvalování a vyhlašování realizace* bezpečnostní politiky včetně základního personálního obsazení a stanovení rolí a odpovědností v oblasti bezpečnosti provádí tajemník úřadu.

Pro bezpečnost IS jsou přijata následující organizační opatření:

- definování bezpečnostního managementu s pravomocemi a odpovědnosti,
- definování manažera bezpečnosti oblasti ICT s pravomoci a odpovědnosti,
- definování odpovědnosti a povinností uživatelů IS ÚMČ.

6.4. Bezpečnostní management

- Funkce bezpečnostního managementu v oblasti bezpečnosti informací stanovuje způsob zajištění bezpečnosti informací

- navrhuje a prosazuje zavedení bezpečnostních opatření do praxe

- plánuje a provádí přezkoumávání dokumentů souvisejících s bezpečností informací z hlediska jejich použitelnosti a aktuálnosti a následně navrhuje jejich úpravy

- členy bezpečnostního managementu jmenuje a odvolává tajemník Úřadu.

Bezpečnostní management se schází podle potřeby Manažer bezpečnosti oblasti OIN vytváří zápis ze schůze.

6.4.1 Složení bezpečnostního managementu

- Gestor správy bezpečnosti
- Koordinátor oblastí procesů
- Manažer bezpečnosti informačních aktiv a IT
- Manažer oblasti (za danou oblast)

6.4.2 Funkce podílející se na řízení bezpečnosti ISVS

- bezpečnostní správce HW a SW systémů
- bezpečnostní správce HW a SW prostředků
- bezpečnostní správce IT systémů

- bezpečnostní správce webu
- bezpečnostní správce firewallu
- manažer fyzické a technické bezpečnosti
- interní audit bezpečnosti informací
- pověřenec pro ochranu osobních údajů (GDPR)
- gestor správy bezpečnosti

6.4.3 Úkoly v rámci bezpečnosti informací

- Gestor správy bezpečnosti je nejvyšším řídícím orgánem, v podmínkách Úřadu městské části je to tajemník úřadu, popř. jeho zástupce.

- Manažer bezpečnosti informačních aktiv a informačních technologií je odpovědný za bezpečnost informací v rámci IS celého Úřadu a dohlíží na její dodržování, koordinuje činnost bezpečnostního fóra, koordinuje školení zaměstnanců v oblasti bezpečnosti informací, dohlíží na provádění změn, připomínkuje změny směrnic a změny další navazující dokumentace, prochází auditní logy, řeší bezpečnostní incidenty a provádí jejich vyhodnocování. Má odborné znalosti v oblasti IT a prokazatelnou znalost normy ČSN ISO/IEC 27001 (bezpečnost informací). V rámci svých pracovních povinností musí být většinu času k zastižení (e-mailem, telefonem), aby byl k dispozici např. v případě výskytu závažného bezpečnostního incidentu. Má delegovanou pravomoc rozhodnutí v zásadních otázkách týkající se bezpečnosti informací. Pravidelně reportuje vedení Úřadu o stavu bezpečnosti informací v organizaci.

- Manažer bezpečnosti oblastí procesů zajišťuje realizaci stanovených požadavků Úřadu městské části Praha 5 na bezpečnost informací s dalšími odbory odbory v rámci organizace a dodavateli informačních a komunikačních služeb. Komunikuje se zástupcem Úřadu, seznamuje jej s navrhovanými řešeními a náročností jejich realizace. Navrhuje možnosti řešení bezpečnostních opatření.

- Manažer oblasti fyzické a technické bezpečnosti zajišťuje případnou realizaci organizačních a technických opatření. Koordinuje realizaci navrhovaných opatření v rámci již zavedených procesů a aktiv úřadu. Kontroluje zpracování provozních řádů a jejich aktualizace. Zpracovává zprávy o mimořádných událostech, jejich řešení, prosazuje opatření k mimořádným událostem a krizovým situacím.

- Bezpečnostní správce zajišťuje bezpečnost informací z technického hlediska, zavedení bezpečnostních opatření připomínkuje z hlediska použitých technologií, řeší bezpečnostní události. Má odborné znalosti v oblasti IT (pravidelně se seznamovat s nejnovějšími trendy a technologiemi v oblasti bezpečnosti informací) a prokazatelnou znalost normy ČSN ISO/IEC 27001 (bezpečnost informací).

- Interní auditor bezpečnosti informací je odpovědný za prověření souladu systému bezpečnosti informací s požadavky normy, stanovenými cíli a dalšími požadavky (např. smluvními či legislativními) a zhodnocení efektivity zavedeného systému. V rámci svých pracovních povinností plánuje a realizuje interní audity, výsledky auditů reportuje vedení Úřadu, upozorňuje na rizikové faktory v oblasti bezpečnosti informací. Má odborné znalosti v oblasti IT, prokazatelnou znalost normy ČSN ISO/IEC 27001(bezpečnost informací) a ČSN EN ISO 19011 (norma pro audit systému řízení).

Podrobné složení bezpečnostního managementu je popsáno v Příloze č. 1.

6.5. Způsob plnění požadavků na bezpečnost

Za plnění konkrétních bezpečnostních požadavků odpovídá pro každý ISVS zástupce architekta ICT systému a to v rámci outsourcingu-správce (administrátor) konkrétního ISVS.

Jeho povinností je dbát na to, aby při běžném provozu informačního systému byly dodržovány postupy stanovené pro splnění bezpečnostních požadavků.

Tyto postupy mohou být různého charakteru, nejčastěji však jde o:

- zákonné normy,
- interní směrnice úřadu (provozní řád, bezpečnostní politika,…),
- doporučení dodavatele ISVS.

6.6. Plnění bezpečnostních požadavků při implementaci nového ISVS

Řízení bezpečnosti při implementaci nového ISVS je opět nedílnou součástí konkrétního projektu. Za splnění jednotlivých bezpečnostních požadavků, které jsou součástí projektové dokumentace, odpovídá vedoucí projektu. Plnění pak provádí projektový tým, respektive jeho jednotliví členové odpovědní za realizaci dílčích projektových úloh.

Důležitou součástí řízení bezpečnosti při implementaci nového ISVS je projektová dokumentace, týkající se oblasti bezpečnosti.

Jedná se zejména o:

- smlouvy (se zaměstnanci a externími subjekty),
- předávací a akceptační protokoly,
- interní směrnice úřadu,
- zápisy ze schůzí organizačních složek projektu,

6.7. Vyhodnocování řízení bezpečnosti ISVS

Vyhodnocování řízení bezpečnosti ISVS se děje formou prověrek a testů. Proces řídí bezpečnostní správce, který při jejich provádění spolupracuje se správcem (administrátorem) konkrétního ISVS.

Bezpečnostní prověrka je konána pro každý ISVS nejméně 1x ročně obvykle na pokyn bezpečnostního správce. Dále může být vykonána mimořádně (mimo obvyklý termín) na pokyn bezpečnostní managementu nebo bezpečnostního správce.

Bezpečnostní prověrka může mít formu:

- kontroly dodržování organizačních postupů (interních směrnic,…),
- kontroly logovacích souborů,
- kontroly provozních deníků,
- kontroly přístupových práv k ISVS,

- pokusu o uložení nekorektních dat,
- simulace pokusu o neoprávněný přístup k ISVS.

O průběhu a výsledcích bezpečnostní prověrky se provádí zápis, který je součástí provozní dokumentace oddělení OIN a správy sítě úřadu.

7. Vyhodnocování dodržování IK

Sledování (a pravidelné vyhodnocování) dodržování zásad stanovených v Informační koncepci je proces, který napomáhá k plnění dlouhodobých cílů Úřadu městské části Praha 5. Vyhodnocování je pak důležitou činností při vlastním provozu IS ÚMČ.

Vyhodnocování dodržování Informační koncepce probíhá vždy 1x ročně. O výsledku vyhodnocení se zhotovuje zápis, který je součástí dokumentace IS ÚMČ.

7.1. Popis procesu vyhodnocování dodržování IK

Vyhodnocování dodržování Informační koncepce provádí pracovní skupina ve složení:

- Gestor správy bezpečnosti
- Interní auditor
- Zastupitel MČ
- Zástupci Architekta ICT systému

Pracovní skupina může být v případě potřeby rozšířena o odborné pracovníky jak z řad zaměstnanců úřadu, tak o externí spolupracovníky.

Pracovní skupina provádí vyhodnocování v následujících oblastech a jejím cílem je zjistit zda:

- aktuální verze IK obsahuje aktuální a pravdivý popis všech používaných ISVS a provozních systémů s vazbou na ISVS (včetně plánovaných změn),
- aktuální verze IK obsahuje všechny záměry na pořízení nových ISVS,
- požadavky na bezpečnost a kvalitu jsou jednotlivými agendami respektovány a plněny,
- plnění požadavků na bezpečnost a kvalitu příznivě ovlivňuje plnění dlouhodobých cílů v těchto oblastech,
- při pořizování nových ISVS (a při provádění změn) jsou uplatňovány zásady uvedené v IK.
- postupy a zásady stanovené v IK nejsou v rozporu s jinými vnitro organizačními směrnicemi se vztahem k IS ÚMČ (Provozní řád IS, Bezpečnostní politika,…),
- postupy a zásady stanovené v IK jsou skutečně v praxi dodržovány,
- nedostatky zjištěné při posledním vyhodnocování dodržování IK byly odstraněny,

- jsou dodržovány zásady financování IS ÚMČ uvedené v IK,
- jsou dodržovány zásady provádění aktualizace IK,
- jsou s aktuálním zněním IK seznámeni všichni pracovníci úřadu, pro které je tento dokument relevantní.

Vyhodnocení probíhá pro každou výše uvedenou oblast zvlášť a ve stejném duchu je i pořízen zápis o vyhodnocování. Při zjištěných nedostatcích je zároveň stanoven způsob jejich odstranění včetně uvedení termínu a osob odpovědných za jejich odstranění.

Konečná verze zápisu je schválena a podepsána všemi osobami, které se na vyhodnocování podílely. Schválená verze je pak dohodnutým způsobem zpřístupněna příslušným pracovníkům úřadu.

7.2. Postupy při provádění změn IK

Udržování Informační koncepce v aktuálním stavu je základní předpoklad splnění zákonných povinností při realizaci dlouhodobého řízení IS ÚMČ.

7.3. Role a odpovědnosti

Při procesu provádění změn IK plní zásadní role následující útvary a pracovníci:

Pracovník odpovědný za aktualizaci Informační koncepce,

který je odpovědný za finální podobu dokumentu IK a za udržování stanoveného způsobu provádění změn včetně archivace jednotlivých verzí dokumentace IK.

Pracovník odpovědný za dodržování Informační koncepce,

který navrhuje změny IK na základě výsledků vyhodnocování dodržování IK.

Oddělení OIN a správy sítě,

které má přehled o všech používaných ISVS a provozních systémů s vazbou na ISVS.

Pracovní skupina pro vyhodnocování dodržování IK,

která (mimo jiné) provádí kontrolu aktuálnosti IK a navrhuje postupy k odstranění zjištěných nedostatků.

7.4. Popis procesu provádění změn IK

Řízení změn v IS ÚMČ je vždy dokumentováno. Stejné povinnosti proto podléhá i provádění změn Informační koncepce. Ke změně Informační koncepce může dojít z rozličných důvodů, ať organizačních, legislativních nebo technických.

Nejčastěji dochází ke změnám Informační koncepce z následujících důvodů:

Změna v organizační struktuře úřadu.

Při organizačních změnách dochází k přesunu kompetencí, popř. vykonávaných činností mezi jednotlivými organizačními jednotkami (odbory, oddělení). Mohou vznikat nové organizační jednotky, další mohou zanikat. Pakliže se provedená organizační změna týká osob či útvarů, kterým jsou přiřazeny určité odpovědnosti v rámci Informační koncepce, je nutné přistoupit k aktualizaci IK. Za provedení těchto změn je odpovědný Odbor OIN

Pořízení nového ISVS (provozního systému s vazbou na ISVS)

Při pořizování nového ISVS se postupuje podle postupů popsaných v příslušných kapitolách tohoto dokumentu. Každému pořízení ISVS předchází vypracování (a schválení) záměru na pořízení a zpracování projektové dokumentace.

Změna v ISVS

Změnou zde rozumíme ty změny, které mají za „následek“ změnu funkčnosti, změnu rozsahu zpracovávaných dat nebo poskytovaných služeb. Veškeré změny jsou dokumentovány a stávají se součástí provozní dokumentace ISVS. Za úplnost provozní dokumentace zodpovídá administrátor příslušného ISVS.

Za změnu se naopak nepovažují provozní zásahy, jako oprava chyb software a podobné činnosti.

Provádění změn v ISVS se děje v režimu tzv. *změnového řízení*.

Nejprve musí být vypracován návrh na změnu ISVS, který obsahuje důvod vzniku požadavku, soupis požadavků na změnu, analýzu současného a cílového stavu ISVS. Dále je navržen způsob realizace provedení změny včetně časového harmonogramu a odhadu nákladů. Návrh na změnu může být předložen organizační jednotkou, která zajišťuje provoz ISVS, popřípadě oddělením OIN a správy sítě.

Ve fázi realizace změny ISVS je pak stanovován závazný harmonogram činností, schvalovány použité nástroje a určeny postupy pro testování provedených změn.

Ukončení provozu ISVS

Z různých důvodů může být rozhodnuto o ukončení provozu ISVS. Obvykle se tak děje při přesunu vykonávaných činností mezi složkami veřejné správy nebo při nahrazení jednoho ISVS druhým. Návrh na ukončení provozu ISVS může být předložen organizační jednotkou, která zajišťuje provoz ISVS, popřípadě oddělení OIN a správy sítě.

V každém případě ukončení provozu je stanoven časový harmonogram ukončení provozu. Důležitým krokem je i stanovení způsobu jak bude nakládáno s daty ISVS a jak bude naloženo s programovým vybavením a s provozní dokumentací. Následně jsou definovány lhůty pro skartaci a likvidaci dokumentace, dat a datových nosičů. Za dodržení všech stanovených postupů odpovídá oddělení OIN a správy sítě.

8. Financování IS úřadu

Základním zdrojem pro financování IS ÚMČ je schválený rozpočet. Veškerý provoz a rozvoj informačního systému musí být v souladu s danými rozpočtovými pravidly. Schvalování rozpočtu provádí Zastupitelstvo MČ Praha 5.

Výše celkového ICT rozpočtu je dána souhrnem provozních a investičních nákladů během kalendářního roku. Za přípravu rozpočtu IS ÚMČ je odpovědné oddělení OIN a správy sítě, které příslušné finanční částky zařadí do návrhu rozpočtu na příští rok.

Financování IS ÚMČ může být v některých případech financováno i z různých dalších zdrojů, jako jsou např. různé dotační tituly. Získané finanční částky jsou pak zařazovány do rozpočtu městské části pomocí rozpočtových změn.

9. Útvar odpovědný za dodržování IK

Za realizaci informační koncepce, tzn. na naplňování dlouhodobých cílů v oblasti informatiky, provoz ISVS a provozních systémů s vazbami na ISVS, dodržování postupů stanovených v Informační koncepci a odstraňování nedostatků při vyhodnocování dodržování Informační koncepce je odpovědný Manažer bezpečnosti informačních aktiv a informačních technologií (vedoucí odboru).

Dodržování Informační koncepce s sebou nese povinnost plnit různé zákonné povinnosti, tak jak stanovuje aktuální právní rád České republiky. Za splnění těchto zákonných povinností je rovněž odpovědné oddělení OIN a správce sítě.

…….

tajemník **Bc. Jozef Žebera**

Přílohy:

Příloha č. 1 – Složení bezpečnostního managementu