Informační koncepce Plzeňského kraje 2021-2026

podle zákona č. 365/2000 Sb.

Verze 2.0

Zpracoval	*Odbor informatiky KÚPK*
Schválil	*Ing. Eliška Pečenková, vedoucí odboru informatiky KÚPK* *Mgr. Jiří Leščinský, ředitel KÚPK*

Datum vydání:	**01. 12. 2021**

Terminologie

Termín (zkratka)	Definice
Informační koncepce (IK)	Dokument, ve kterém orgány veřejné správy stanoví své dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných ISVS a vymezí obecné principy pořizování, vytváření a provozování ISVS viz § 5a odst. 1 zákona o ISVS.
Informační systém (IS)	Informačním systémem se rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností viz § 2 písm. b) zákona o ISVS.
Informační systém o datových prvcích (IS o DP)	Aplikace Informační systém o datových prvcích poskytuje oficiální informace o datových prvcích informačních systémů veřejné správy, slouží k vyhlašování datových prvků a zveřejňování číselníků. Datové prvky vyhlášené v Informačním systému o datových prvcích jsou pro orgány veřejné správy a vazby jejich informačních systémů závazné.
Informační systém o informačních systémech veřejné správy (IS o ISVS)	Aplikace Informační systém o informačních systémech slouží ke sběru a poskytování informací o informačních systémech veřejné správy (ISVS). Jedná se o základní informace o ISVS a informace o dostupnosti ISVS.
Informační systém veřejné správy (ISVS)	Informační systémy veřejné správy jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Jsou jimi i informační systémy zajišťující činnosti podle zvláštních zákonů viz § 3 odst. 1 zákona o ISVS.
Provozní IS (PIS)	Provozním informačním systémem se rozumí informační systém zajišťující informační činnosti nutné pro vnitřní provoz příslušného orgánu VS, například účetnictví, správu majetku, a nesouvisející bezprostředně s výkonem veřejné správy viz § 2 písm. u) zákona o ISVS.
Provozní dokumentace (PD)	Dokumentace informačního systému veřejné správy, která popisuje funkční a technické vlastnosti informačního systému viz § 2 písm. x) zákona o ISVS.
Významný IS (VIS)	Informační systém, klasifikovaný jako významný podle § 2 zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

Obsah

1 Identifikace Informační koncepce

1.1 Základní údaje Informační koncepce

Název organizace	Plzeňský kraj		
IČ	70890366		
Typ organizace	kraj – vyšší územně samosprávný celek		
Adresa	Škroupova 18, 306 13 Plzeň		
Kontakt	www.plzensky-kraj.cz, posta@plzensky-kraj.cz		
Datum zpracování	22. 11. 2021		
Platnost	01. 12. 2021 – 30. 11. 2026		
Aktuální verze	2.0		
Schválení	Ing. Eliška Pečenková, vedoucí odboru informatiky KÚPK dne Mgr. Jiří Leščinský, ředitel KÚPK dne		
Soubor	IK KUPK v2.0 (11-2021 v1).docx		
Umístění	Sdílený disk – odbor informatiky		
Počet stran	43	Počet příloh	2

Tabulka č. 1: Základní údaje o Informační koncepci.

1.2 Verze Informační koncepce

V dílčích článcích této kapitoly jsou popsány všechny verze Informační koncepce chronologicky od aktuálně platné až po nejstarší – původní verze Informační koncepce.

Drobné změny Informační koncepce schvaluje vedoucí odboru informatiky. Jsou odlišeny změnou čísla verze (z v1 se stane v2), nová verze je platná od okamžiku jejího schválení, konec platnosti se neposouvá.

V případě zásadních změn, nebo pokud skončí platnost celé Informační koncepce, vydá odbor informatiky novou Informační koncepci. Tuto změnu předkládá odbor informatiky ke schválení řediteli KÚPK.

1.2.1 Aktuální verze Informační koncepce

Označení verze	**2.0**	Datum vzniku	22.11.2021
Schválení	Ing. Eliška Pečenková, vedoucí odboru informatiky KÚPK dne Mgr. Jiří Leščinský, ředitel KÚPK dne		
Platnost verze	01. 12. 2021 – 30. 11. 2026		
Počet stran	43	Počet příloh	2
Změny	Aktualizace seznamu a charakteristik ISVS a PIS Doplnění a aktualizace řízení kvality ISVS Doplnění a aktualizace řízení bezpečnosti ISVS Aktualizace zákonných povinností a odpovědností Drobné aktualizace ostatních kapitol		
Soubor	IK KUPK v2.0 (11-2021 v1).docx		
Umístění	Sdílený disk – odbor informatiky		

Tabulka č. 2: Údaje o aktuální verzi Informační koncepce.

1.2.2 Historie verzí Informační koncepce

1.2.2.1 Verze 1

Označení verze	**1**	Datum vzniku	12. 08. 2016
Schválení	Ing. Eliška Pečenková, vedoucí odboru informatiky KÚPK dne 23. 08. 2016. Mgr. Jiří Leščinský, ředitel KÚPK dne 23. 08. 2016.		
Platnost verze	01. 09. 2016 – 31. 08. 2021		
Počet stran	43	Počet příloh	2
Změny	Kompletně přepracovaná Informační koncepce na základě vývoje informační společnosti, změn legislativy, výsledků projektů podpořených dotací ze SF EU v programovacím období 2007-2013 a výhledu na programovací období 2014-2020.		

Tabulka č. 3: Údaje o verzi 1 Informační koncepce.

2 Kontext Informační koncepce

Informační koncepce Plzeňského kraje (dále jen „PK“) je dokumentem zaměřeným na dlouhodobé cíle a obecné principy související se správou a rozvojem jednotlivých ISVS.

Zásady a postupy, uvedené v této Informační koncepci, jsou závazné pouze pro ISVS ve správě Krajského úřadu PK (dále jen „KÚPK“) a pro provozní IS, které mají vazbu na ISVS v rozsahu této vazby. V ostatních případech mají zásady a postupy, uvedené v tomto dokumentu, pouze sílu doporučení a je na rozhodnutí osoby, která za danou oblast Informační koncepce zodpovídá, zda bude v daném konkrétním případě vyžadovat jejich plnění v definovaném rozsahu či nikoli.

Informační koncepce popisuje:

- charakteristiky všech spravovaných ISVS a předpokládané změny,
- záměry na pořízení nebo vytvoření nových ISVS,
- dlouhodobé cíle v oblasti řízení kvality,
- dlouhodobé cíle v oblasti řízení bezpečnosti,
- postupy při vyhodnocování dodržování Informační koncepce,
- postupy při provádění změn Informační koncepce,
- zásady pro správu ISVS s postupy pro jejich naplnění,
- financování oblasti ISVS,
- útvar/funkční zařazení zaměstnance odpovědného za naplňování Informační koncepce
- hodnocení naplnění cílů, principů a zásad IK ČR.

Legislativně se Informační koncepce řídí především zákonem č. 365/2000 Sb., o informačních systémech veřejné správy (ISVS), v aktuálním znění, a jeho prováděcí vyhláškou č. 529/2006 Sb., o dlouhodobém řízení ISVS.

Dále jsou při provozování ISVS respektovány především následující předpisy:

- zákon č. 250/2017 Sb., o elektronické identifikaci
- zákon č. 111/2009 Sb., o základních registrech
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- zákon č. 110/2019 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů,
- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,

Další právní normou, která upravuje postavení krajských úřadů je zákon č. 129/2000 Sb., o krajích.

Významný vliv na celkovou koncepci budování IS krajského úřadu má také zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek.

Významným řídícím dokumentem pro tvoru Informační koncepce je Program rozvoje Plzeňského kraje 2014+ a zejména Informační strategie Plzeňského kraje. Za stěžejní v celostátním měřítku pak lze považovat tyto dokumenty a projekty:

- Digitální Česko
- Informační koncepce České republiky (Digitální veřejná správa)
- Klientsky orientovaná veřejná správa ČR 2030 – Koncepce rozvoje veřejné správy na období let 2021–2030

3 Informační systémy ve správě Krajského úřadu Plzeňského kraje

V této části Informační koncepce jsou identifikovány informační systémy veřejné správy (ISVS), provozní informační systémy (PIS) s vazbou na informační systémy veřejné správy a ostatní provozní informační systémy.

Z rozhodnutí KÚPK jsou zde zařazeny také významné informační systémy (VIS) podle zákona o kybernetické bezpečnosti.

Seznam významných IS spravovaných nebo provozovaných KÚPK je veden online v nástroji HelpDesk v elektronické podobě (http://helpdesk.plzensky-kraj.cz). Za aktuálnost elektronického seznamu aplikací v IS HelpDesk odpovídá vedoucí oddělení aplikací a databází OIT KÚPK. V příloze č. 1 je uveden výstup z tohoto IS, platný ke dni zpracování této verze Informační koncepce.

V následující tabulce je uveden pouze výčet ISVS, a provozních IS vyjmenovaných v §1 odst4 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „ZoISVS“). Dílčí charakteristiky ISVS i vyjmenovaných PIS jsou v příloze č.2 Informační koncepce.

Název / poznámka	Identifikace IS[1]	typ IS
Agendio / elektronický agendový systém	*1428*	*ISVS, PIS (§1, odst 4b ZoISVS), VIS*
AthenA / elektronický systém spisové služby	*1427*	*ISVS, VIS*
AZ Pro / informační systém pro řízení a rozvoj lidských zdrojů a odměňování	*[53]*	*PIS (§1, odst 4a ZoISVS), VIS*
ePUSA	*3699*	*ISVS*
HESS – Hostovaná spisová služba	*1911*	*ISVS*
Hledáček / přístupový systém k ISZR	*8986*	*ISVS*
Navision / ekonomický systém	*[138]*	*PIS (§1, odst 4c ZoISVS), VIS*
Poštovní systém – MS Outlook / systém elektronické pošty	*[129]*	*PIS (§1, odst 4d ZoISVS), VIS*
Portál Plzeňského kraje / webový portál	*[98]*	*PIS (§1, odst 4b ZoISVS), VIS*

Tabulka č. 4: Přehled ISVS, VIS a provozních IS s vazbou na ISVS

[1] U ISVS identifikátor ISVS v RPP působnostním, u PIS interní identifikátor IS

4 Záměry na pořízení nebo vytvoření nových IS

Plzeňský kraj v současnosti neplánuje pořízení nebo vybudování nového ISVS nebo nové vazby provozního IS na existující ISVS. Plzeňský kraj v současnosti neplánuje pořízení nebo vybudování nového VIS.

Další kroky budou koordinovány se strategií MV při realizaci strategie e-governmentu a s Informační strategií Plzeňského kraje.

5 Řízení kvality ISVS

Informační systém Plzeňského kraje je rozsáhlý – přistupuje k němu cca 450 interních uživatelů z řad zaměstnanců KÚPK a další tisíce externích uživatelů (pracovníci zřizovaných organizací, obecní úřady, občané aj.). Správa informačního systému takového rozsahu klade nároky nejen na hardware a síťovou infrastrukturu, ale celkem logicky i na dlouhodobé řízení.

5.1 Dlouhodobé cíle kvality ISVS

V oblasti řízení kvality ISVS jsou stanoveny následující cíle:

- Soulad IS PK s platnou legislativou ČR a EU a jeho budování s důrazem na transparentnost.
- Vysoká kvalita dat IS PK – především zajištění integrity a konzistence dat a jejich důvěryhodnosti (tj. aktuálnosti a správnosti).
- Vysoká kvalita služeb, zajišťovaných IS PK – vysoká míra použitelnosti a užitná hodnota pro uživatele, pomoc s dosahováním cílů kraje.
- Vysoká kvalita technických a programových prostředků – zajištěná dostupnost IS PK pro uživatele a jeho bezpečnost a spolehlivost.

Pro VIS platí uvedené cíle obdobně.

Specifické cíle v oblasti řízení kvality IS jsou uvedeny v následující tabulce, a to v členění do tří výše uvedených hlavních cílů, s tím, že Soulad IS PK s platnou legislativou ČR a EU je cílem, který se promítá do všech specifických cílů i činností KUPK. U každého cíle je dále uveden atribut kvality IS, ke kterému cíl směřuje.

Oblast kvality	Název cíle	Popis cíle	Požadavek kvality
Zajištění kvality dat	Včasná aktualizace údajů	Všechny údaje vedené primárně KUPK budou aktualizovány v nejbližší možné době po jejich změnách. Podobně nové údaje by se měly objevit v IS s minimální prodlevou.	E, Q
	Kontroly dat proti primárním registrům	Všechny údaje, které vede KUPK a které mají prvotní uložení v jiných systémech (zejména tzv. základních registrech), by měly být kontrolovány proti těmto registrům.	E
	Kontroly obsahu dat	Ve všech systémech budou využity algoritmy pro vnitřní kontrolu obsahu a integrity dat, a to na všech úrovních (databáze, aplikační logika, vstupní formuláře apod.).	E
Zajištění kvality ICT služeb	Zajištění služeb v provozní době	ICT služby budou provozovány v závislosti na kritičnosti aplikace.	Q
	Zajištění úrovně dostupnosti služeb	Bude zajištěna definovaná úroveň dostupnosti služeb, a to souborem technických a procesních řešení v IT oblasti.	Q
	Monitoring služeb	Zajištění systému provozního monitoringu služeb s návazností na procesy řízení incidentů.	Q, S
	Řízení incidentů a problémů	Systematické řízení řešení výpadků kvality IS (dodávky služeb apod.). Příjem a řešení chybových hlášení, identifikace příčin, přiřazení řešitele a řešení hlášení. Systematická identifikace problémů a jejich řešení.	Q, S

Oblast kvality	Název cíle	Popis cíle	Požadavek kvality
Zajištění kvality techn. a program. prostředků	Pokrytí agend TPP	Agendy i podpůrné činnosti jsou podporovány IS v ekonomické výhodné míře.	S
	Uživatelsky přívětivé GUI	Tvorba základního standardu UI; ergonomie, standardizace a přívětivost UI.	Q, S
	Nízká chybovost aplikací	Zajištěna kvalita aplikací prostřednictvím přípravy a realizace testovacích scénářů, dílčích i akceptačních testů a zajištění podpory dodavatelů.	E, Q, S
	Výkonnostní parametry aplikací	Aplikace s rychlými odezvami, běžící na určených moderních a kvalitních technologiích.	Q, S

Tabulka č. 5: Cíle kvality ISVS

5.2 Požadavky na kvalitu ISVS

Požadavky na kvalitu pro oblast ICT a její řízení jsou uvedené v následující tabulce:

Cíl kvality	Popis požadavku	Platí pro
Včasná aktualizace údajů	Agendy i podpůrné činnosti jsou podporovány IS v ekonomické výhodné míře.	Všechny IS
	Data jsou online ukládána centrálně (pouze jednou) a jsou ve vhodném rozsahu meziaplikační sdílena.	Všechny IS
Kontroly dat proti primárním registrům	IS napojeny na základní registry.	Vybrané IS
Kontroly obsahu dat	IS obsahují při ukládání kontroly obsahu a formátu dat, uživatelsky přívětivě reagují na neshody.	Všechny IS
	IS obsahují při ukládání kontroly relací dat i jejich integrity a konzistence, tyto kontroly probíhají při vkládání / editaci.	Vybrané IS
Zajištění služeb v provozní době	Evidence portfolia služeb na základě business požadavků na provozní dobu služeb.	Všechny IS
	Zajištění dostupnosti služeb v rozsahu provozní doby.	Všechny IS
Zajištění úrovně dostupnosti služeb	Řízení specifikace požadavků koncového zákazníka / gestora, jejich ukotvení a nastavení jejich parametrů.	Všechny IS
	Technické zajištění služeb dostatečnou infrastrukturou a jejího technického řešení.	Vybrané IS
Monitoring služeb	Funkční systém monitoringu ICT služeb a technologické i komunikační infrastruktury na jejich pozadí.	Vybrané IS
	Funkční systém příjmu hlášení incidentů.	Všechny IS
Řízení incidentů a problémů	Nastavený a funkční systém Helpdesku pro řešení incidentů i problémů.	Všechny IS
	Nastavení procesy incident a problem managementu, vč. definice řešitelských skupin.	Všechny IS
Pokrytí agend TPP	IS podporují výkon procesů jednotlivých agend a podpůrných procesů.	Všechny IS
Uživatelsky přívětivé GUI	Dodržení standardů uživatelského rozhraní.	Vybrané IS
	Evidence koncových zákazníků jednotlivých služeb, řízení evidence jejich požadavků na změny i chybových hlášení, identifikace zákaznických potřeb a kontrola jejich spokojenosti.	Všechny IS

Cíl kvality	Popis požadavku	Platí pro
Nízká chybovost aplikací	Řízení plánování a nasazení releasů IS.	Nové IS
	Systematické řízení testování a konečného vyhodnocování.	Nové IS
	Zajištěna podpora aplikace ze strany dodavatele.	Vybrané IS
Výkonnostní parametry aplikací	Rychlé odezvy UI aplikací.	Vybrané IS
	Využití standardizovaného, moderního prostředí pro fungování aplikací.	Všechny IS

Tabulka č. 6: Požadavky na kvalitu ISVS

Obecné požadavky na kvalitu jsou definovány z pohledu primárních aktiv, tedy dat ISVS, přičemž technické a programové prostředky a služby jsou (ve smyslu podpůrných a technických aktiv) nutnou podmínkou pro jejich zajištění. Požadavky na kvalitu jsou stanoveny takto:

Požadavky	Kvalita			Specifikace
	dat	TPP	služeb	
Bezvadnost (E)	✔	✔	✔	IS nemají vady, nedostatky či nedodělky, které ztěžují či přímo zabraňují užívání systému ze strany uživatelů či způsobují poškození dat.
Kvalitativní parametry (Q)	✔	✔	✔	Znaky či vlastnosti aktiv informačních systémů, které jsou pro uživatele důležité (z pohledu dostupnosti, odezvy atp.). Čím mají informační systémy lepší vlastnosti, tím jsou považovány za kvalitnější.
Stabilita (S)	✔	✔	✔	Zajištění stability informačních systémů v čase, a to prostřednictvím systému řízení kvality informačních systémů (mnoho změn v IT prostředí vede k nespokojenosti uživatelů a zvýšení rizika nefunkčnosti jednotlivých systémů)

Tabulka č. 7: Obecné požadavky na kvalitu ISVS

5.3 Plán řízení kvality

5.3.1 Provozní činnosti

Činnost	**Požadavek**	**Popis činnosti**	**Termín**
Management konfigurace	E, Q, S	Dokumentováním aktualizace a správa komponent služeb a TPP, zajištění dostupnosti konfigurační matice relevantním rolím	průběžně
Management incidentů a problémů	E, Q, S	Systematické řízení řešení výpadků kvality IS (dodávky služeb apod.). Příjem a řešení chybových hlášení, identifikace příčin, přiřazení řešitele a řešení hlášení. Systematická identifikace problémů a jejich řešení.	průběžně
Management změn	E, Q, S	Systematické řešení změnových požadavků, návrh řešení, realizace, analýzy dopadů a implementace do provozního prostředí.	průběžně
Management nasazení	E, Q, S	Řízení plánování a nasazení releasů IS, řízení vývoje, testování a konečného vyhodnocování	průběžně
Management úrovně služeb	E, Q	Řízení specifikace požadavků koncového zákazníka, jejich ukotvené a nastavení jejich parametrů	průběžně

Činnost	Požadavek	Popis činnosti	Termín
Management kapacit	E, Q, S	Řízení zdrojů pro zajištění služeb a infrastruktury, zejm. kapacit infrastruktury (vč. monitoringu apod.), ale i kapacit lidských zdrojů a dalších.	průběžně
Management kontinuity a dostupnosti služeb	E, S	Průběžná analýza dopadů výpadků kritických služeb IT (analýza rizik), stanovení a aktualizace plánů obnovy, vyhodnocování jejich efektivity a jejich další aktualizace	průběžně
Management vztah s odběrateli	E, Q, S	Evidence koncových zákazníků jednotlivých služeb, řízení evidence jejich požadavků na změny i chybových hlášení, identifikace zákaznických potřeb a kontrola jejich spokojenosti. Fungující víceúrovňová podpora uživatelů v pracovní době	průběžně
Řízení dodavatelů	E, Q, S	Evidence externích dodavatelů, jejich vazeb na dodávky služeb a komponent, monitorování jejich výkonnosti, identifikace slabých míst smluvních vztahů a jejich vylepšování a případné řízení změny dodavatelů služeb a komponent. Projektové řízení vztahů s dodavateli ICT	průběžně
Reportování služeb	Q	Systematické měření kvalitativních parametrů služeb a TPP a jejich vyhodnocování.	průběžně
Řízení kvality dat	E, Q	Monitorování dat, tj. kontrola zadávaných hodnot, notifikace uživatele v reálném čase na základě stanovených pravidel a postupů, jejich čistění dle složitějších a sofistikovanějších metod, ověřování dat ověřují vůči daným interním či externím číselníkům, doplňování dat za využití externích, volně přístupných zdrojů informací. ostatků.	průběžně

Tabulka č. 8: Plán řízení kvality – provozní činnosti

5.3.2 Rozvojové činnosti

Činnost	Požadavek	Popis činnosti	Termín
Rozšíření a údržba evidence HW – plánů obnovy	E, Q, S	Evidence HW a plán jejich obnovy bude průběžně aktualizována.	Průběžně k 31.8.
Systém klíčových uživatelů	Q, S	Školení klíčových uživatelů, jejich činností apod.	31.12.2022 průběžně
Integrace Portálu občana	E, Q, S	Portál občana integrovat na systém Vyjadřování k existenci sítí	31.3.2022
Modernizace ePUSA	E, Q, S	Sběr požadavků na modernizaci systému ePUSA	30.6.2022
Sběr zpětné vazby	E, S	Analýza možnost pro sběr zpětné vazby občanů i zaměstnanců (ředitel KUPK, 31.12.2022)	31.12.2022
Projektová a architektonická kancelář	E, Q, S	Analýza možností vytvoření projektové a architektonické kanceláře a vzniku metodiky Enterprise architektury (ředitel KUPK, 31.12.2022)	31.12.2022
Rozvoj Change managementu	E, S	Analýza potřeb a využití, případně požadavky na směrnici change managementu sumarizovat do specifické směrnice (vedoucí odboru informatiky, 31.12.2022)	31.12.2022
Implementace procesního řízení a řízení kvality	Q, S	Provést analýzu možností implementace procesního řízení na celý úřad ve spojitosti s implementací Metodického pokynu MVČR pro řízení kvality ve služebních úřadech (ředitel KUPK, 30.6.2022)	30.6.2022

Tabulka č. 9: Plán řízení kvality – rozvojové činnosti

5.3.3 Kontrola a vyhodnocování naplňování požadavků

Činnost	Požadavek	Popis činnosti	Termín
Stanovení dlouhodobých cílů kvality informačních systémů	E, Q, S	Vymezení a transformace dlouhodobých cílů kvality informačních systémů přes dílčí věcné cíle (požadavky na kvalitu) do informačních projektů a jejich začlenění do portfolia informačních projektů. Plánování rozpočtu informačních projektů – provádí vedoucí odboru informatiky ve spolupráci s jednotlivými odděleními OIT	1 x 2 roky
Implementace dlouhodobých cílů kvality informačních systémů	E, Q, S	Realizace dlouhodobých cílů kvality informačních systémů v rámci řízení portfolia informačních projektů – provádí projektový tým v závislosti na termínech řešení a s ohledem na postupu řešení jednotlivých úloh (v oblasti životního cyklu IS) a provádí vedoucí odboru informatiky ve spolupráci s jednotlivými odděleními OIT (v oblasti řízení ICT KUPK) Za následné dodržení požadavků na kvalitu konkrétního IS je zodpovědný společně správce IS a věcný garant IS, kteří spolu úzce spolupracují. Celkově za kvalitu celého IS PK zodpovídá vedoucí odboru informatiky KÚPK	průběžně
Vyhodnocení dlouhodobých cílů kvality informačních systémů	E, Q, S	Vyhodnocení dlouhodobých cílů kvality informačních systémů v rámci vyhodnocení informační koncepce – provádí tým, jmenovaný vedoucím odboru informatiky KÚPK, případně může být proveden formou outsourcingu externím dodavatelem. Z prověření se vytváří zápis, který obdrží vedoucí odboru informatiky, správce IS a garant IS. Při běžném provozu ISVS provádí pracovník odpovědný za řízení kvality 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 a garanty jednotlivých IS. 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 IS). Zbylé požadavky pak podléhají pravidelnému vyhodnocování. Vyhodnocení řízení kvality jako celku provádí pracovníci odboru informatiky, pověření vedoucím odboru. Vyhodnocení se provádí vždy v rámci vyhodnocování souladu provozování IS PK s platnou Informační koncepcí, případně častěji dle potřeby. Součástí vyhodnocení je i revize dlouhodobých cílů kvality a jejich případná aktualizace. Vyhodnocení může být podnětem k vydání nové verze Informační koncepce.	1 x 2 roky průběžně
Revize dlouhodobých cílů kvality informačních systémů	E, Q, S	Revize dlouhodobých cílů kvality informačních systémů (vyřazení naplněných cílů, příp. aktualizace stávajících cílů a stanovení nových cílů).	1 x 2 roky

Tabulka č. 10: Plán řízení kvality – kontrolní činnosti

6 Řízení bezpečnosti

Strategickým dokumentem v oblasti řízení bezpečnosti je Bezpečnostní politika IS KÚPK. 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 KÚPK rovněž obecně definuje bezpečné používání informačních zdrojů.

6.1 Dlouhodobé cíle v oblasti řízení bezpečnosti ISVS

Základními bezpečnostními cíli je zajištění následujících stavů a činností:

1) trvalé a kvalitní zajištění dostupnosti, důvěrnosti, integrity a autentizace dat,
2) ochrana dat a prostředků ISVS,
3) zajištění bezpečné komunikace s okolím.

Pro VIS platí uvedené cíle obdobně.

Dlouhodobé cíle v oblasti řízení bezpečnosti informačních systémů veřejné správy, které korespondují s požadavky na kvalitu popsanými níže, jsou stanoveny (v souladu s vyhláškou č. 529/2006 Sb.) ve třech hlavních oblastech:

- Zajištění bezpečnosti dat, která jsou v ISVS zpracovávána
- Zajištění bezpečnosti technických a programových prostředků
- Zajištění bezpečnosti služeb, které jsou prostřednictvím ISVS poskytovány

Specifické cíle v oblasti řízení bezpečnosti IS jsou uvedeny v následující tabulce, a to v členění do tří výše uvedených hlavních cílů. U každého cíle je dále uveden požadavek bezpečnosti IS, ke kterému cíl směřuje.

Oblast bezpečnosti	Název cíle	Popis cíle	Požadavek bezpečnosti
Zajištění bezpečnosti dat	Údržba systému řízení bezpečnosti dat	Údržba a rozvoj systému řízení bezpečnosti dat a informací.	A, C, I, L
	Provádění kontrol a auditů	Dokumentace požadavků relevantních právních a regulatorních předpisů a smluvních závazků. Provádění a dokumentování kontrol dodržování stanovených pravidel.	L
	Zajištění organizační bezpečnosti	Řízení přístupových práv uživatelů k datům, řízení bezpečnosti dodavatelů, ochrana autorizačních údajů ze strany všech uživatelů.	C, I, L
	Zajištění fyzické bezpečnosti	Ochrana neoprávněného vstupu, poškození, kompromitace aktiv.	C, I, L
Zajištění bezpečnosti ICT služeb	Řešení kybernetických bezpečnostních událostí a incidentů	Příprava prostředí pro vyhodnocení kybernetických bezpečnostních událostí, systém řešení kybernetických událostí a incidentů.	A, C, I, L

Oblast bezpečnosti	Název cíle	Popis cíle	Požadavek bezpečnosti
	Zajištění kontinuity služeb	Dokumentace strategie a cílů řízení kontinuity. Stanovení postupů pro provedení protiopatření.	A, I
	Využívání bezpečnostních SW nástrojů	Zajištění vstupů do infrastruktury KUPK prostřednictvím SW nástrojů, logování činností uvnitř sítě.	C, L
Zajištění bezpečnosti techn. a program. prostředků	Řízení provozu a komunikace informačních systémů	Zajištění bezpečného provozu IS, stanovení provozních pravidel a postupů, plán a následná tvorba/aktualizace provozně technické dokumentace IS, detekce kybernetických událostí.	A, C, I, L
	Řízení aktiv a rizik informačních systémů	Stanovení a prosazení pravidel pro ochranu aktiv podle jejich klasifikace. Spolehlivé mazání a likvidace aktiv, zpracování a zavedení plánu zvládání rizik.	A, C, I
	Zajištění bezpečnosti lidských zdrojů	Proškolené lidské zdroje, řízení využívání TPP dle platných bezpečnostních pravidel.	C, I, L
	Řízení akvizice, vývoje a údržby informačních systémů	Stanovení bezpečnostních požadavků na informační systémy.	C, I
	Zajištění aplikační bezpečnosti	Realizace bezpečnostních testů aplikací (vč. penetračních).	A, C, I

Tabulka č. 11: Cíle bezpečnosti ISVS

6.2 Požadavky na bezpečnost ISVS

Pro naplnění výše uvedených cílů byly v oblasti řízení bezpečnosti stanoveny následující požadavky:

Cíl bezpečnosti	Popis požadavku	Platí pro
Údržba systému řízení bezpečnosti dat	Údržba aktuálního souboru dokumentace systému řízení bezpečnosti informací.	Všechny IS
	Dodržování postupů dle dokumentace, tvorba výstupů.	Vybrané IS
Provádění kontrol a auditů	Realizace auditů a kontrol systému bezpečnosti informací, interních smluvních, technických i procesních auditů.	Vybrané IS
Zajištění organizační bezpečnosti	Zpracování dokumentace o bezpečnostních rolích, nastavení systému přístupu k datům a jeho kontrola.	Všechny IS
	Jednotný způsob autorizace a autentizace, prioritně prostřednictvím MS AD a SSO PK	Všechny IS
	Využití dodavatelů při rozvoji, provozu ICT nebo zajištění bezpečnosti podmíněno smlouvou včetně ujednání o bezpečnosti informací.	Všechny IS
Zajištění fyzické bezpečnosti	Zavedení a využívání prostředků fyzické bezpečnosti – mechanické zábranné, EZS, vstupní systémy, kamerové systémy, UPS, klimatizace, …	Vybrané IS
Řešení kybernetických bezpečnostních události a incidentů	Příprava prostředí pro vyhodnocení kybernetických bezpečnostních událostí.	Vybrané IS
	Hlášení kybernetických bezpečnostních incidentů, jejich řešení, vč. dokumentace systému zvládání kybernetických bezpečnostních incidentů.	Vybrané IS
Zajištění kontinuity služeb	Udržování procesu řízení kontinuity, havarijních plánů a plánů obnovy. Existence systému pravidelného zálohování a archivace dat.	Vybrané IS

Cíl bezpečnosti	Popis požadavku	Platí pro
Využívání bezpečnostních SW nástrojů	Využití SW nástrojů pro ochranu integrity komunikačních sítí (rozhraní vnější a vnitřní sítě), ochranu před škodlivým kódem, zaznamenávání činností informačních systémů, jejich uživatelů a správců.	Vybrané IS
Řízení provozu a komunikace	Stanovení provozních pravidel a postupů.	Všechny IS
	Používán bezpečných komunikačních cest	Všechny IS
	Detekce kybernetických bezpečnostních událostí a jejich vyhodnocení.	Vybrané IS
Řízení aktiv a rizik informačních systémů	Identifikace aktiv a jejich garantů, jejich klasifikace a aktualizace.	Vybrané IS
	Hodnocení rizik, plán jejich zvládání.	Vybrané IS
Zajištění bezpečnosti lidských zdrojů	Proškolené lidské zdroje. Kontrola dodržování pravidel. Vrácení svěřených prostředků při ukončení pracovního poměru. Zpracování a zavedení plánu rozvoje bezpečnostního povědomí.	Všechny IS
	Ukládání auditních záznamů o změnách údajů v IS (jejich původci) a zajištění bezpečnosti logů.	Vybrané IS
Řízení akvizice, vývoje a údržby informačních systémů	IS nastaveny dle definovaných bezpečnostních požadavků na informační systémy, koordinace nastavení v rámci systému IT, vlastní řízení aplikace bezpečnostních požadavků při pořízení i rozvoji IS.	Nové a aktualizované IS
Zajištění aplikační bezpečnosti	Realizace bezpečnostních testů aplikací před uvedením do provozu.	Vybrané IS

Tabulka č. 12: Požadavky na bezpečnosti ISVS

Obecné požadavky na bezpečnost jsou definovány z pohledu primárních aktiv, tedy dat ISVS, přičemž technické a programové prostředky a služby jsou (ve smyslu podpůrných a technických aktiv) nutnou podmínkou pro jejich zajištění. Požadavky na bezpečnost ISVS jsou stanoveny takto:

Požadavek	**Bezpečnost**			**Specifikace**
	dat	**TPP**	**služeb**	
Dostupnost (A)	✔	✔	✔	Data a informace jsou dostupné v okamžiku jejich potřeby v požadovaném rozsahu a kvalitě.
Důvěrnost (C)	✔	✔	✔	K datům a informacím mají přístup pouze oprávněné osoby), jsou chráněné před neoprávněným užitím.
Integrita (I)	✔	✔	✔	U dat a informací je zajištěna jejich správnost a úplnost a jsou stanovena práva pro jejich změnu.
Auditovatelnost (L)	✔	✔	✔	Dohledatelnost aktivit ve vztahu k datům a informacím (log aktivit uživatelů).

Tabulka č. 13: Obecné požadavky na bezpečnost ISVS

6.3 Plán řízení bezpečnosti

6.3.1 Provozní činnosti

Činnost	Požadavek	Popis činnosti	Termín
Údržba systému řízení bezpečnosti dat	A, C, I, L	Postupné zavedení systému řízení bezpečnosti dat a informací. Vyhodnocování a údržba systému.	průběžně
Řízení aktiv informačních systémů	A, C, I, L	Identifikování a ohodnocení primárních aktiv, určení garantů aktiv. Stanovení a prosazení pravidel pro ochranu aktiv podle jejich klasifikace. Spolehlivé mazání a likvidace aktiv.	průběžně
Řízení rizik aktiv informačních systémů	A, C, I, L	Identifikace a hodnocení rizik primárních aktiv (významných) informačních systémů. Určení a schválení zbytkových rizik, vytvoření zprávy o hodnocení rizik a jejich pravidelná aktualizace. Zpracování prohlášení o aplikovatelnosti. Zpracování a zavedení plánu zvládání rizik.	průběžně
Hodnocení a aktualizace bezpečnostní politiky informačních systémů	A, C, I, L	Stanovení pravidel pro základní oblasti kybernetické bezpečnosti. Hodnocení účinnosti politik a jejich aktualizace.	průběžně
Zajištění organizační bezpečnosti	C, I, L	Udržování dokumentace o bezpečnostních rolích (bezpečnostní politika), nastavení systému a jeho kontrola. Ochrana autorizačních údajů ze strany všech uživatelů.	průběžně
Řízení bezpečnosti dodavatelů	A, C, I, L	Využití dodavatelů při rozvoji, provozu ICT nebo zajištění bezpečnosti podmíněno smlouvou včetně ujednání o bezpečnosti informací	průběžně
Zajištění bezpečnosti lidských zdrojů	C, I, L	Poučení lidských zdrojů o bezpečnosti informací. Kontrola dodržování pravidel. Vrácení svěřených prostředků při ukončení pracovního poměru. Zpracování a zavedení plánu rozvoje bezpečnostního povědomí.	průběžně
Řízení provozu a komunikace informačních systémů	A, C, I, L	Detekce kybernetických bezpečnostních událostí a jejich vyhodnocení. Zajištění bezpečného provozu, stanovení provozních pravidel a postupů.	průběžně
Řízení přístupu k informačním systémům	C, I, L	Nastavení, řízení a kontrola systému řízení přístupu k informačním systémům a datům.	průběžně
Řízení akvizice, vývoje a údržby informačních systémů	A, C, I, L	Stanovení bezpečnostních požadavků na informační systémy, koordinace nastavení v rámci systému IT, vlastní řízení.	průběžně
Řešení kybernetických bezpečnostních události a incidentů	A, C, I, L	Příprava prostředí pro vyhodnocení kybernetických bezpečnostních událostí. Neprodlené hlášení každého kybernetického bezpečnostního incidentu. Dokumentace systému zvládání kybernetických bezpečnostních incidentů.	průběžně
Zajištění kontinuity činností informacích systémů	A, C, I, L	Systémové řízení kontinuity. Stanovení postupů pro provedení protiopatření.	průběžně
Provádění kontrol a auditů	L	Dokumentace požadavků relevantních právních a regulatorních předpisů a smluvních závazků. Provádění a dokumentování kontrol dodržování stanovených pravidel.	průběžně
Zajištění fyzické bezpečnosti	A, C, I, L	Ochrana neoprávněného vstupu, poškození, kompromitace aktiv. Zavedení prostředků fyzické bezpečnosti – mechanické zábranné, EZS, vstupní systémy, kamerové systémy, UPS, klimatizace, …	průběžně

Činnost	Požadavek	Popis činnosti	Termín
Využívání požadovaných bezpečnostních SW nástrojů	A, C, I, L	Ochrana integrity komunikačních sítí (rozhraní vnější a vnitřní sítě) prostřednictvím SW nástroje. Ověřování identity uživatelů prostřednictvím SW nástroje. Řízení přístupových oprávnění prostřednictvím SW nástroje. Ochrana před škodlivým kódem prostřednictvím SW nástroje. Zaznamenávání činností informačních systémů, jejich uživatelů a správců prostřednictvím SW nástroje. Detekce kybernetických bezpečnostních událostí prostřednictvím SW nástroje.	průběžně
Zajištění aplikační bezpečnosti	A, C, I, L	Realizace bezpečnostních testů aplikací přístupných z vnější sítě před uvedením do provozu.	průběžně
Využívání kryptografických prostředků	C	Údržba směrnice o kryptografii. Ochrana přenosu po komunikačních sítích, uložení na mobilní zařízení nebo vyměnitelná média.	průběžně
Údržba požadované bezpečnostní dokumentace	A, C, I, L	Údržba, vyhodnocování a aktualizace dokumentů, zejm. Bezpečnostní politika.	průběžně

Tabulka č. 14: Plán řízení bezpečnosti – provozní činnosti

6.3.2 Rozvojové činnosti

Činnost	Požadavek	Popis činnosti	Termín
Nové TC3	A, C, I	Vybudování nového datového centra	31.12.2024
Školící prostředí	A, C, I	Doplnění školícího prostředí u klíčových IS	31.12.2024
Rozšíření infrastruktury	D	Rozšíření komunikační infrastruktury kraje	31.12.2026
Modernizace DTM	C, I	Rozvoj systému digitální technické mapy	31.12.2023
Kvalita datového fondu	A, C, I	Rozvoj datového fondu	31.12.2024

Tabulka č. 15: Plán řízení bezpečnosti – rozvojové činnosti

6.3.3 Kontrola a vyhodnocování naplňování požadavků

Činnost	Požadavek	Popis činnosti	Termín
Stanovení cílů bezpečnosti a dlouhodobých cílů bezpečnosti informačních systémů	A, C, I, L	Vymezení dlouhodobých cílů bezpečnosti informačních systémů a jejich transformace přes požadavky na bezpečnost do informačních projektů a jejich začlenění do portfolia informačních projektů – provádí bezpečnostní manažer IS, Cíle bezpečnosti jsou stanoveny na základě Bezpečnostní dokumentace KÚPK, ve které jsou detailně rozpracovány.	1 x 2 roky
Stanovení požadavků na bezpečnost	A, C, I	Na základě cílů bezpečnosti stanoví bezpečnostní správce IS ve spolupráci s manažerem bezpečnosti IS požadavky na bezpečnost, jež povedou k naplnění cíle, a předá je vedoucímu odboru informatiky odpovědnému za rozvoj IS. Jednotlivé požadavky na bezpečnosti jsou pak zapracovány do Plánu bezpečnosti spolu se stanovením termínu plnění.	1 x ročně

Činnost	Požadavek	Popis činnosti	Termín
Implementace dlouhodobých cílů bezpečnosti informačních systémů a požadavků na bezpečnost	A, C, I, L	Realizace dlouhodobých cílů bezpečnosti informačních systémů v rámci řízení portfolia informačních projektů. Jednotlivé požadavky na bezpečnost mohou být implementovány prostřednictvím několika bezpečnostních opatření, odpovědnost za implementaci požadavků na bezpečnost, spolu se způsobem jejich implementace je definována v Plánu bezpečnosti, za který odpovídá manažer bezpečnosti IS. Dokončení implementace požadavku hlásí manažer bezpečnosti IS vedoucímu odboru informatiky.	průběžně
Prověrka dodržování požadavků na bezpečnost	A, C, I, L	Provádí ji externí organizace dle výsledků výběrového řízení a v souladu s plánem snižování rizik, když impuls k prověrce dává plán řízení rizik, který stanovuje mimo jiné vždy roční harmonogram provádění jednotlivých opatření, včetně zodpovědnosti a vyčlenění zdrojů. Při prověrce se prověřuje konkrétní implementace jednoho nebo více požadavků na IS KÚPK a z prověření se vytváří zápis, který obdrží manažer bezpečnosti IS a vedoucí odboru informatik. Prověrka se provádí pravidelně jedenkrát ročně, při zásadní změně IS nebo technických prostředků je součástí změnového řízení a akceptačních testů.	1 x ročně
Vyhodnocení cílů řízení bezpečnosti	A, C, I, L	Na základě prověrky provede manažer bezpečnosti IS též revizi cílů řízení bezpečnosti a jejich aktualizaci, vyřadí se implementované a prověřené požadavky na bezpečnost a vytvoří se nové Způsob kontroly a hodnocení řízení bezpečnosti je definován v Bezpečnostní dokumentaci KÚPK.	1 x ročně
Vyhodnocení dlouhodobých cílů bezpečnosti informačních systémů	A, C, I, L	Vyhodnocení dlouhodobých cílů bezpečnosti informačních systémů v rámci vyhodnocení informační koncepce. Vyhodnocení může být podnětem k vydání nové verze IK.	1 x 2 roky
Revize dlouhodobých cílů bezpečnosti informačních systémů	A, C, I, L	Revize dlouhodobých cílů bezpečnosti informačních systémů (vyřazení naplněných cílů, příp. aktualizace stávajících cílů a stanovení nových cílů).	1 x 2 roky

Tabulka č. 16: Plán řízení bezpečnosti – kontrolní činnosti

7 Zásady a postupy pro správu ISVS

7.1 Zásady a postupy pro pořizování a vytváření ISVS

Zásady a postupy, platné pro pořizování a vytváření ISVS, se aplikují i v případě změny ISVS.

7.1.1 Vypracování záměru nového ISVS

Před zahájením pořízení nového IS musí být zpracován záměr nového IS, a to u drobných záměrů jako požadavek v IS HelpDesk, u rozsáhlých záměrů pak musí být záměr rozpracován v samostatném dokumentu Koncepce záměru IS – záměr zpracovávají pracovníci odboru informatiky a schvaluje jej vedoucí odboru informatiky KÚPK, za úzké součinnosti věcného správce (věcné vymezení, požadavky) a technického správce (koncepce řešení).

Rozhodnutí o rozsahu záměru (tj. zda jde o rozsáhlý záměr a je tedy nutné vypracovat Koncepci záměru IS) je v kompetenci vedoucího odboru informatiky, který rozhodne především na základě rozsahu předpokládaných dopadů, očekávané finanční náročnosti a délky, složitosti a způsobu realizace.

Záměr na pořízení, vytvoření nebo změnu drobného IS bude popsán v IS HelpDesk jako „Problém s programem“. Ke každému takovému požadavku musí být vedeno:

- definování potřeby IS, včetně předpokládané finanční náročnosti a analýzy zdrojů pro jeho pořízení
- analýza výchozího stavu
- stanovení cílového stavu
- požadavky na kvalitu a bezpečnost IS
- plán přechodu (návrh transformace z výchozího do cílového stavu)
- analýza důsledků

Struktura dokumentu Koncepce záměru IS pro rozsáhlé IS obsahuje kromě výše uvedených položek v Helpdesku i koncepci řešení, zejm. pak:

- zásady
- průběh instalace
- vazby na ostatní systémy
- administraci
- definici a popis oprávnění
- harmonogram

7.1.2 Pořizování nového ISVS

Záměr na pořízení ISVS je vypracován vnitřním útvarem úřadu (odbor, oddělení) obvykle na základě požadavku vedoucího odboru, ředitele úřadu, člena Rady kraje či Zastupitelstva kraje, popř. zřízené komise či výboru.

Schválení záměru doporučuje pracovní skupina, jejíž složení 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, který se řídí dle vnitřních pravidel KÚPK o projektovém řízení.

Pro každý pořizovaný nebo aktualizovaný IS určí vedoucí odboru informatiky pracovníka odboru informatiky, zodpovědného za dodávku tohoto IS (dále odpovědný pracovník odboru informatiky).

Zároveň ředitel úřadu na návrh odboru informatiky jmenuje garanta IS z odboru KÚPK, do jehož kompetence IS věcně spadá.

V případě pořizování IS je povinností vytvořit zadávací dokumentaci pro výběr vhodného řešení v následujícím předpokládaném rozsahu:

- funkční specifikace,
- rozsah analýzy a koncepce nasazení,
- požadavky na provozní dokumentaci IS,
- požadavky na projektové řízení u dodavatele,
- požadavky na kvalitu, vyplývající z dlouhodobých cílů řízení kvality,
- požadavky na bezpečnost, vyplývající z dlouhodobých cílů řízení bezpečnosti,
- požadavky na testování,
- podmínky akceptace.

Odpovědný pracovník odboru informatiky je zodpovědný za to, že zadávací dokumentace bude zpracována v dále uvedené kvalitě a rozsahu. Na tomto úkolu úzce spolupracuje především s garantem IS.

Zadávací dokumentaci nového nebo aktualizovaného IS schvaluje vedoucí odboru informatiky, případně další osoby v souladu s příslušnými interními předpisy KÚPK (zejm. směrnicí o veřejných zakázkách) a Plzeňského kraje a platnou legislativou.

7.1.2.1 Funkční specifikace

Funkční specifikace musí obsahovat minimálně požadavky na:

- funkcionalitu IS, požadavky na jeho jednotlivé funkce,
- integraci s ostatními částmi IS,
- vstupní a výstupní data,
- legislativní požadavky,
- technologické požadavky,
- ostatní uživatelské požadavky.

7.1.2.2 Rozsah analýzy a koncepce nasazení

V případě, že rozsah nebo složitost pořizovaného IS znemožňuje detailní popis zadání před vyhlášením veřejné zakázky, může být Zadávací dokumentace zpracována pouze v omezené míře podrobnosti. Povinnou požadovanou součástí dodávky pak musí být provedení analýzy a na jejím základě zpracování dokumentu Koncepce nasazení, která bude odsouhlasena před zahájením vlastní implementace IS a která upřesní chybějící části zadání.

Rozhodnutí o potřebě provedení analýzy a zpracování Koncepce nasazení je v kompetenci vedoucího odboru informatiky.

7.1.2.3 Požadavky na provozní dokumentaci IS

Odpovědný pracovník odboru informatiky zodpovídá za to, že součástí dodávky bude kompletní provozní dokumentace v souladu s požadavky vyhlášky č. 529/2006 Sb., o dlouhodobém řízení ISVS.

7.1.2.4 Požadavky na projektové řízení u dodavatele

Implementační projekty budou řízeny prostřednictvím projektového řízení. Uchazeč v rámci své nabídky musí jasně specifikovat projektovou strukturu a metodiku, podle které budou projekty řízeny.

7.1.2.5 Požadavky na kvalitu, vyplývající z dlouhodobých cílů řízení kvality

Požadavky na kvalitu vyplývají z dlouhodobých cílů řízení kvality – viz kap. 5.1.

7.1.2.6 Požadavky na bezpečnost, vyplývající z dlouhodobých cílů řízení bezpečnosti

Požadavky na bezpečnost vyplývají z dlouhodobých cílů řízení bezpečnosti – viz kap. 6.

7.1.2.7 Požadavky na testování

Požadavky na testování budou vycházet z rozsahu systému, počtu poskytovaných služeb apod. Požadavky budou buď součástí Zadávací dokumentace, nebo součástí Koncepce nasazení.

Z testování musí být vypracován protokol z testování, který je podkladem pro akceptaci.

7.1.2.8 Podmínky akceptace

Součástí akceptace je kontrola shody implementované funkcionality se stanovenými akceptačními kritérii, které budou buď součástí Zadávací dokumentace, nebo součástí Koncepce nasazení.

Výsledkem akceptace musí být akceptační protokol, obsahující výsledek akceptace a případný výčet připomínek s termínem jejich odstranění.

7.1.3 Vytváření nového ISVS prostřednictvím zaměstnanců

Požadavky na dokumentaci procesu vytváření ISVS jsou shodné s požadavky na dokumentaci procesu pořízení ISVS. Vedoucí odboru informatiky nebo vedoucí oddělení, které vytváření zajišťuje, může pro konkrétní případ stanovit potřebu další dokumentace nad tento základní rámec.

Pro vytvořený ISVS musí vzniknout provozní dokumentace v plném rozsahu, požadovaném vyhláškou č. 529/2006 Sb., tedy

- bezpečnostní dokumentace
- systémová příručka
- uživatelská příručka

Provozní dokumentace bude umístěna následovně:

- bezpečnostní dokumentace – u bezpečnostního správce
- systémová příručka – v Helpdesku u dané aplikace (bude primárně držena v elektronické podobě)
- uživatelská příručka – v nápovědě aplikace (bude primárně držena v elektronické podobě)

7.2 Zásady a postupy pro provozování ISVS

7.2.1 Zajištění provozu a údržby ISVS

7.2.1.1 Zásady a postupy pro vlastní zajištění provozu a údržby

Vytváření a údržba provozní dokumentace

Pracovník odboru informatiky, odpovědný za dodávku IS a správce IS zodpovídají za naplnění požadavku dodání provozní dokumentace v rámci dodávky IS.

Zajištění souladu provozování s IK a provozní dokumentací

Uživatelé budou prokazatelně seznámeni se svými povinnostmi zakotvenými v provozní dokumentaci. Tato činnost bude opakována při každé relevantní změně provozní dokumentace. Za tuto činnost zodpovídá vedoucí odboru informatiky, který může tímto úkolem pověřit správce IS nebo jiného pracovníka odboru informatiky.

7.2.1.2 Zásady a postupy vyhodnocování souladu provozování

Vyhodnocování souladu provozní dokumentace s požadavky Vyhlášky

Prověření obsahu provozní dokumentace na vyhláškou předepsané součásti je součástí akceptační procedury dodávky nového IS nebo nové verze IS. Za toto vyhodnocení zodpovídá pracovník odboru informatiky, který zodpovídá za dodávku IS (odpovědný pracovník odboru informatiky) a správce IS. Výsledek vyhodnocení je uveden v akceptačním protokolu, kde případné neshody budou uvedeny jako připomínky z akceptace s dohodnutým termínem odstranění.

Vyhodnocování souladu provozování ISVS s Informační koncepcí a provozní dokumentací

Vyhodnocování probíhá vždy nejpozději 1x za 24 měsíců, řídí jej a za jeho průběh zodpovídá vedoucí odboru informatiky. Z vyhodnocení je vypracován zápis, obsahující výsledek vyhodnocení, nalezené neshody a úkoly nutné pro jejich odstranění.

7.2.1.3 Stanovení povinností osob v oblasti provozu a údržby

Pracovníci KÚPK dodržují pravidla pro práci s ISVS, která jsou specifikována v provozní dokumentaci jednotlivých IS. Při zjištění problémů nahlásí podnět na HelpDesk, případně kontaktují odpovědného pracovníka z odboru informatiky a dále postupují dle jeho pokynů.

7.2.2 Řízení změn v ISVS

Pod pojmem provádění změn v IS se rozumí kvalitativní změny, spojené se změnami funkčnosti nebo datového rozhraní (např. potřeba rozšíření funkcionality, změna datových rozhraní, reagování na novelizaci právních předpisů).

Zásady a postupy pro řízení změn v ISVS jsou shodné se zásadami a postupy pro pořízením nového ISVS (kap. 7.1.1).

Provádění změn je třeba odlišit od běžné údržby ISVS. Změnou je chápán takový zásah do IS, který významným způsobem mění jeho funkcionalitu, rozsah či strukturu udržovaných dat, technologii nebo vazby či rozhraní na jiné ISVS. Za změnu není považováno provádění činností, které vedou k zachování funkcí ISVS v požadovaném a nezměněném stavu (například opravy chyb, bezpečnostní záplaty apod.). Rozsah činností údržby, které nejsou považovány za změnu, budou upřesněné v provozní dokumentaci ISVS. V případě, že z povahy činnosti jasně nevyplývá, zda jde o změnu ISVS nebo o jeho údržbu, je závazné posouzení správce daného IS.

Řízení změn v ISVS musí být vždy dokumentováno. Konkrétní pravidla pro řízení změn budou upřesněna v provozní dokumentaci každého ISVS, a to v závislosti na jeho významu a rozsahu. Není-li v provozní dokumentaci stanoveno jinak, zodpovídá za dokumentaci správce daného IS. Při přebírání nové verze ISVS dohlíží správce IS na zajištění:

- aktualizace provozní dokumentace,
- proškolení uživatelů ISVS a správce ISVS (je-li to nutné),
- zálohování a převedení dat,
- otestování funkcionality ISVS a dat,
- akceptace.

7.2.3 Ukončení činnosti ISVS

Při ukončování činnosti ISVS se bude tento proces a jeho dokumentace řídit stejnými pravidly jako proces řízení změn ISVS, tedy bude zpracován dokument Koncepce záměru IS, kde bude stanoveno rovněž:

- jak bude naloženo s daty (převod, archivace, skartace, …),
- jak bude naloženo s ISVS,
- naplánování harmonogramu ukončení,
- zajištění kontinuity služeb.

8 Způsob financování ISVS

Základním zdrojem pro financování IS Plzeňského kraje je schválený rozpočet KÚPK. Veškerý provoz a rozvoj informačního systému musí být v souladu s danými rozpočtovými pravidly. Schvalování rozpočtu provádí Zastupitelstvo Plzeňského kraje.

Výše celkového rozpočtu je dána souhrnem provozních a investičních nákladů během kalendářního roku. Za přípravu rozpočtu IS je odpovědný odbor informatiky KÚPK, který příslušné finanční částky zařadí do návrhu rozpočtu na příští rok.

Financování IS může být v některých případech financováno i z různých dalších zdrojů, jako jsou např. různé dotační tituly, především ze strukturálních fondů EU. Získané finanční částky jsou pak zařazovány do rozpočtu kraje pomocí rozpočtových změn.

8.1 Financování záměrů na pořízení nebo vytvoření nových ISVS

Pořízení nového ISVS je realizováno zejména na základě výběrového řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Při čerpání a případných změnách rozpočtových prostředků KÚPK postupuje v souladu se zákonem č. 218/2000 Sb., o rozpočtových pravidlech, a vyhláškou č. 560/2006 Sb., o účasti státního rozpočtu na financování programů reprodukce majetku. Nakládání s ISVS, které jsou majetkem KÚPK, je prováděno v souladu se zákonem č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích.

Financování s příspěvkem Evropské unie

Financování pořizování nových IS může probíhat také s finančním příspěvkem Evropské unie (využití operačních programů strukturálních fondů určených pro podporu modernizace veřejné správy a rozvoj informační společnosti ve veřejné správě), případně z finančních prostředků, určených vládou ČR na výzkum a vývoj.

8.2 Financování správy ISVS

Financování správy provozovaných ISVS provádí KÚPK z provozních finančních prostředků v souladu se zákonem č. 218/2000 Sb., o rozpočtových pravidlech v aktuálním znění.

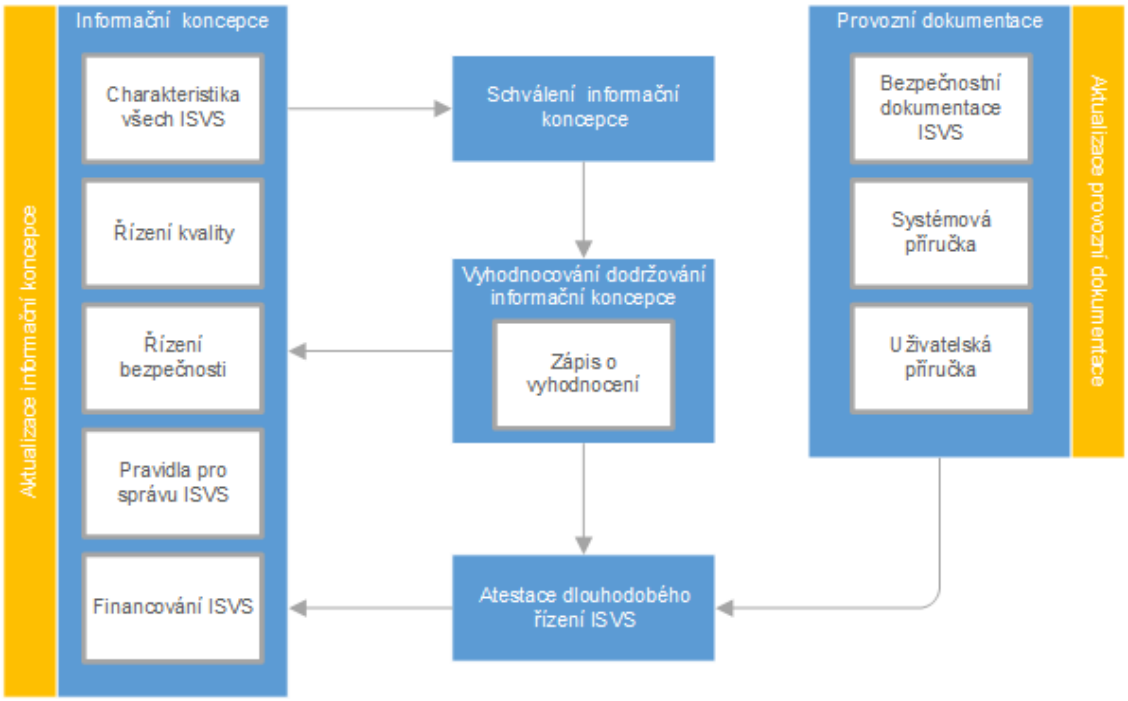
8.3 Řídící kontrola a další působení kontrolních orgánů

Nedílnou součástí řízení financování ISVS, potažmo ICT jako celku, je i vnitřní kontrolní systém KÚPK, který je reprezentován řídící kontrolou dle zákona č. 320/2001 Sb., o finanční kontrole ve všech fázích:

- předběžná kontrola před vznikem závazku nebo nároku,
- předběžná kontrola po vzniku závazku nebo nároku,
- kontrola průběžná a
- kontrola následná.

9 Naplňování Informační koncepce

Proces dlouhodobého řízení ISVS lze demonstrovat na následujícím obrázku:



Obrázek č. 1: Naplňování Informační koncepce

Za naplňování Informační koncepce jsou považovány činnosti, prostřednictvím kterých dojde k:

- praktickému naplnění postupů a zásad uvedených v Informační koncepci,
- udržování Informační koncepce v aktuálním stavu,
- pravidelnému vyhodnocování dodržování Informační koncepce a k realizaci opatření pro odstranění zjištěných nedostatků.

Pro zajištění praktického naplnění postupů a zásad uvedených v Informační koncepci je třeba stanovit osobní odpovědnosti za jednotlivé oblasti, které Informační koncepce řeší. Toto je pro přehlednost provedeno v kap. 10. Dále musí být zajištěna kontrola tohoto naplnění – viz kap. 9.2.

9.1 Postupy při provádění změn Informační koncepce

Provádění změn do Informační koncepce lze rozdělit na čtyři činnosti:

- včasná detekce změn v oblastech, které se dotýkají Informační koncepce tak, aby byla zajištěna včasná změna Informační koncepce,
- vlastní provedení změny v Informační koncepci, resp. vydání její nové verze,
- schválení změny Informační koncepce, resp. její nové verze,
- příprava nové Informační koncepce v předstihu před ukončením platnosti té stávající.

Uvedené činnosti provádí pracovník, zodpovědný za plnění a aktualizaci Informační koncepce.

9.1.1 Postup pro zajištění včasné změny Informační koncepce

Pro zajištění včasné aktualizace Informační koncepce bude prováděna její revize 1x za dva roky, a to v zodpovědnosti osoby stanovená v kap. 10 (vedoucí odboru informatiky KÚPK).

9.1.2 Postup zápisu změny do dokumentu Informační koncepce

Změny Informační koncepce budou prováděny formou vydání nové verze. Jednotlivé verze budou číslovány dvěma čísly, oddělenými tečkou:

- hlavní číslo verze, které bude odlišovat verze s významnými změnami (např. kompletně přepracované kapitoly, změny zásadních postupů apod.),
- vedlejší číslo verze, které bude odlišovat drobnější změny (např. doplnění nového ISVS, změny v personální oblasti, drobná změna v postupech apod.).

U každé verze se budou sledovat následující atributy:

- číselné označení verze,
- datum vzniku verze,
- datum schválení verze,
- datum počátku platnosti verze,
- název souboru s elektronickou verzí Informační koncepce,
- umístění souboru (na intranetu, sdíleném disku apod.),
- verze souboru obsahujícího schválenou podobu dané verze Informační koncepce,
- počet stran a počet příloh,
- autor verze Informační koncepce, který provedl schválené změny,
- osoba, která schválila verzi Informační koncepce.

Každá verze bude obsahovat tabulku změn oproti verzi předchozí. V této tabulce budou pro každou změnu stručně uvedeny následující informace:

- popis provedené změny,
- odůvodnění změny,
- identifikace místa (příp. více míst) dokumentu (minimálně číslem kapitoly), kterého se změna dotkla.

Přípravu změn do dokumentu Informační koncepce, ať už tvorbu nové nebo akualizaci zajišťuje vedoucí odobru informatiky KÚPK s případnou součinností dalších pracovníků odboru informatiky.

9.1.3 Postup schvalování změny Informační koncepce

Verzi je třeba předložit ke schválení minimálně 2 týdny před požadovaným vstupem v platnost. K nové verzi je třeba přiložit všechny dokumenty, na základě nichž byla verze vytvořena, nebo alespoň odkazy na ně.

S novou verzí budou po jejím schválení prokazatelně seznámeni všichni pracovníci odboru informatiky a dále ostatní pracovníci, kteří mají ve vztahu k Informační koncepci definovanou povinnost (přidělenou roli).

Změnu Informační koncepce schvaluje osoba stanovená v kap. 10.

9.1.4 Postup přípravy nové Informační koncepce

Pracovník odpovědný za plnění a aktualizaci Informační koncepce připraví 2 měsíce před ukončením její platnosti podklady pro rozhodnutí ohledně přípravy nové Informační koncepce. Tyto podklady budou obsahovat:

- vyhodnocení stávající Informační koncepce a její účinnosti (míru naplnění cílů kvality a cílů bezpečnosti) za dobu od jejího vzniku,
- vyhodnocení způsobu vzniku a údržby stávající Informační koncepce a doporučení pro postup tvorby nové Informační koncepce (vlastními silami nebo s využitím externího dodavatele apod.),
- další podklady dle uvážení tohoto pracovníka.

Novou Informační koncepci schvaluje osoba stanovená v kap. 10.

9.2 Postupy při vyhodnocování dodržování Informační koncepce

Vyhodnocování dodržování Informační koncepce je základním kontrolním mechanizmem, zajišťujícím zpětnou vazbu.

Vyhodnocování musí vždy provádět jiný pracovník než ten, který je odpovědný za plnění a aktualizaci Informační koncepce. Totéž platí pro vyhodnocování dílčích oblastí, pro které byla stanovena konkrétní dílčí odpovědnost.

Pro vyhodnocování dodržování Informační koncepce byla stanovena perioda 1 x za 24 měsíců. Tato perioda bude sladěna s periodou aktualizace Informační koncepce tak, aby se opatření přijatá na základě vyhodnocování stala předmětem pravidelné aktualizace Informační koncepce.

Vyhodnocování iniciuje a řídí vedoucí odboru informatiky KÚPK. Pro vyhodnocování dílčích oblastí musí být dodržena výše uvedená nezávislost vyhodnocující osoby na osobě odpovědné za realizaci. Vlastní realizace vyhodnocení bude zajištěna externí společností formou zakázky. Externí společnost bude pro každé vyhodnocení nově vybrána.

Všechny činnosti, jejichž provádění je posuzováno, jsou porovnávány s Informační koncepcí platnou v době, kdy byla daná činnost prováděna.

Vyhodnocování bude probíhat metodou dekompozice na dílčí oblasti a jejich následnou expertní analýzou. Pracovník provádějící vyhodnocení si připraví tabulku, kde bude sledovat výsledky dílčích vyhodnocení jednotlivých oblastí, evidovat zjištěné nedostatky a zapisovat návrhy opatření na jejich odstranění.

9.2.1 Oblasti pro vyhodnocování Informační koncepce

9.2.1.1 Oblast charakteristik informačních systémů veřejné správy

- Informační koncepce obsahuje charakteristiky všech ISVS.
- Informační koncepce obsahuje všechny provozní IS s vazbami na ISVS.
- Charakteristiky současného stavu jsou včas aktualizovány.
- Předpokládané změny IS jsou včas aktualizovány.

9.2.1.2 Oblast záměrů pořízení nebo vytvoření nových ISVS

- Informační koncepce obsahuje všechny záměry nových ISVS.
- Jednotlivé záměry mají vyplněny všechny základní údaje.
- Pro všechny záměry jsou vypracovány charakteristiky nového IS.
- Pro všechny záměry existuje charakteristika výchozího stavu, toto posuzování se provádí u záměrů vytvořených v období od předcházejícího vyhodnocení.

9.2.1.3 Oblast řízení kvality

- Požadavky na kvalitu směřují k naplnění cílů kvality.
- Požadavky na kvalitu jsou jednotlivými IS dodržovány a jsou vyhodnocovány.

- Probíhá prověrka požadavků na kvalitu a vyhodnocení řízení kvality v souladu s plánem řízení kvality.

9.2.1.4 Oblast řízení bezpečnosti

- Požadavky na bezpečnost směřují k naplnění cílů bezpečnosti.
- Požadavky na bezpečnost jsou jednotlivými IS dodržovány a jsou vyhodnocovány.
- Probíhá prověrka požadavků na bezpečnost a vyhodnocení řízení bezpečnosti v souladu s plánem řízení bezpečnosti.

9.2.1.5 Oblast správy ISVS

- Jsou uplatňovány zásady a postupy pro plánování rozvoje ISVS.

Oblast správy ISVS – část pořizování ISVS

- Výběr formy pořizování nového ISVS je prováděn v souladu s příslušnými zásadami a postupy.
- Pro každý nový ISVS je vypracován záměr s požadovanou strukturou a v souladu s požadovanými zásadami a postupy.
- Při pořizování ISVS je vyžadováno naplnění všech oblastí dle Informační koncepce platné v době pořizování ISVS, tyto požadavky jsou zakotveny ve smlouvě.
- Při vytváření ISVS jsou všechny procesy tvorby IS náležitě dokumentovány.
- V případě využití projektového řízení jsou uplatňovány přijaté zásady v této oblasti.

Oblast správy ISVS – část provozování ISVS

- Jsou uplatňovány zásady a postupy pro plánování rozvoje ISVS.
- Jsou uplatňovány zásady a postupy pro zajištění provozu a údržby ISVS.
- Jsou uplatňovány zásady a postupy pro řízení změn ISVS.
- Jsou uplatňovány zásady a postupy pro ukončení činnosti ISVS.

9.2.1.6 Oblast financování ISVS

- Financování ISVS probíhá v souladu se schválenými postupy a platnými předpisy.
- Existuje pravidelně aktualizovaný plán financování ISVS.
- Plán financování ISVS obsahuje dílčí plány financování: záměrů nových IS, naplnění dlouhodobých cílů a správy ISVS.
- Jednotlivé dílčí plány financování jsou tvořeny a aktualizovány v souladu s příslušnými pravidly.

9.2.1.7 Oblast změn Informační koncepce

- Jsou dodržovány termíny periodické aktualizace.
- Významné změny jsou promítány do Informační koncepce i mimo její periodické aktualizace.
- Vydávání nových verzí Informační koncepce probíhá v souladu s danými postupy, verze a v nich zahrnuté změny jsou náležitě dokumentovány a schvalovány.
- Všichni relevantní pracovníci mají k dispozici aktuální platnou verzi Informační koncepce.
- Nejsou používány neplatné verze Informační koncepce.

9.2.1.8 Oblast vyhodnocování dodržování Informační koncepce

- Prováděné vyhodnocení nastalo nejpozději v předepsaném časovém intervalu od minulého vyhodnocení.

- Zápisy z minulých vyhodnocení jsou dostupné obdobně, jako aktuální verze Informační koncepce.
- Opatření přijatá při minulých vyhodnoceních dodržování Informační koncepce byla promítnuta do aktualizované verze Informační koncepce.
- Přijatá opatření jsou uplatňována v praxi.
- Přijatá opatření přinesla předpokládaný účinek – dříve zjištěné nedostatky byly odstraněny nebo se k jejich odstranění směřuje.

9.2.1.9 Oblast definice odpovědností

- Jsou definovány role odpovědné za jednotlivé oblasti realizace Informační koncepce.
- Jsou definovány role odpovědné za jednotlivé oblasti splnění zákonných povinností.

9.2.2 Pravidla pro vytváření zápisu z vyhodnocování Informační koncepce

Z vyhodnocování bude vytvořen zápis. Za jeho vyhotovení zodpovídá pracovník, který řídí vyhodnocování a je určen v kap. 10.

9.2.2.1 Rozsah zápisu z vyhodnocování

Zápisy z vyhodnocování budou identifikovány verzí Informační koncepce, které se týkají, a dále pak pořadovým číslem zápisu. Zápis bude obsahovat následující části:

- identifikační údaje zápisu (verze Informační koncepce, datum počátku platnosti vyhodnocované Informační koncepce, pořadové číslo zápisu),
- identifikace všech pracovníků, kteří vyhodnocení prováděli, a jejich role (jméno, resp. jména, příjmení, útvar nebo externí organizace, funkce),
- záznam o průběhu vyhodnocování dle jednotlivých oblastí (co, jak, kdy a kdo vyhodnocoval),
- poznatky a závěry z vyhodnocování (soupis zjištěných nedostatků, kladná hodnocení apod.),
- soupis přijatých opatření (návaznost na zjištěný nedostatek, obsah opatření, způsob realizace apod.),
- schválení zápisu z vyhodnocení (kdo – jméno, resp. jména, příjmení, útvar nebo externí organizace, funkce a kdy zápis schválil).

9.2.2.2 Postup vyhotovení zápisu z vyhodnocování

Do zápisu se po úvodních identifikačních údajích nejprve zapisuje záznam o průběhu vyhodnocení a poznatky a závěry z něj.

V dalším kroku vedoucí odboru informatiky zajistí zpracování návrhu vhodných opatření, která se spolu s částečným zápisem předloží ke schválení. Schválená opatření jsou poté vložena do zápisu a zápis je uzavřen a předložen ke schválení.

Schválený zápis se zpřístupní a všichni dotčení pracovníci se s ním seznámí obdobným způsobem, jako je to u nové verze Informační koncepce. Opatření s vlivem na obsah Informační koncepce se promítnou v nejbližší řádné aktualizaci Informační koncepce.

10 Funkční zařazení osoby, která řídí provádění činností podle Informační koncepce a zákona o ISVS

Stanovení odpovědností v oblasti dlouhodobého řízení ISVS je nedílnou součástí Informační koncepce. Odpovědnosti lze rozdělit do dvou částí, a to na stanovení odpovědností za:

- realizaci Informační koncepce,
- splnění zákonných povinností.

10.1 Odpovědnost za realizaci Informační koncepce

Odpovědnost za naplnění Informační koncepce je stanovena na odboru informatiky KÚPK.
Dílčí odpovědnosti za jednotlivé oblasti Informační koncepce jsou uvedeny v následující tabulce.

Oblast	Odpovědnost	Náplň oblasti	Četnost
identifikace záměrů na pořízení nových ISVS	pracovníci odboru informatiky KÚPK	Kap. 4 (Kap. 7.1)	Průběžně
schvalování záměrů na pořízení nových ISVS	vedoucí odboru informatiky KÚPK	Kap. 4 (Kap. 7.1)	Při každém požadavku na pořízení nového ISVS
řízení kvality ISVS (stanovování dlouhodobých cílů kvality a konkrétních požadavků na kvalitu IS, sestavení a údržba plánu řízení kvality, vyhodnocování naplnění požadavků a dodržování plánu)	vedoucí odboru informatiky KÚPK	Kap. 5 (Kap. 9.2)	min. 1x za dva roky
řízení bezpečnosti ISVS (stanovování dlouhodobých cílů bezpečnosti a konkrétních požadavků na bezpečnost IS, sestavení a údržba plánu řízení bezpečnosti, vyhodnocování naplnění požadavků a dodržování plánu)	vedoucí odboru informatiky KÚPK	Kap. 6 (Kap. 9.2)	min. 1x za dva roky
koordinace činností v oblasti rozvoje ISVS	vedoucí odboru informatiky KÚPK	Kap. 7.1	Průběžně
řízení postupů při pořizování ISVS (včetně zajištění veřejných soutěží)	vedoucí odboru informatiky KÚPK Řídí se Směrnicí Rady Plzeňského kraje č. 1/2014 - o zadávání veřejných zakázek a Směrnicí odboru informatiky SIT 01-09 Veřejné zakázky malého rozsahu	Kap. 7.1.2	Průběžně
zajištění provozu a údržby ISVS	vedoucí oddělení aplikací a databází	Kap. 7.2.1.1	Průběžně, resp. při změně IS
vyhodnocování dodržování souladu provozování ISVS	vedoucí odboru informatiky KÚPK	Kap. 7.2.1.2	Při změně IS, min. 1x za dva roky

Oblast	Odpovědnost	Náplň oblasti	Četnost
koordinace a vyhodnocování řízení změn	vedoucí odboru informatiky KÚPK	Kap. 7.2.2	Při změně IS
řízení ukončování provozu ISVS	vedoucí odboru informatiky KÚPK	Kap. 7.2.3	Při ukončení činnosti části IS
vytváření a údržba plánu financování ISVS	vedoucí odboru informatiky KÚPK	Kap. 8	Probíhá každoročně v rámci procesu přípravy rozpočtu
schvalování plánu financování ISVS	Zastupitelstvo Plzeňského kraje (v rámci schvalování rozpočtu kraje)	Kap. 8	Probíhá každoročně v rámci procesu přípravy rozpočtu
příprava změn a tvorba nových verzí Informační koncepce	vedoucí odboru informatiky KÚPK	Kap. 9.1	revize min. 1x za dva roky
schvalování změn Informační koncepce a jejích nových verzí	vedoucí odboru informatiky KÚPK a ředitel KÚPK	Kap. 9.1.3	Podle potřeby
příprava nové Informační koncepce před ukončením platnosti stávající	vedoucí odboru informatiky KÚPK	Kap. 9.1.4	2 měsíce před koncem platnosti, min. každých 5 let
provádění vyhodnocování dodržování Informační koncepce a vyhotovení zápisu o něm	vedoucí odboru informatiky KÚPK	Kap. 9.2	1x za dva roky
návrh opatření na základě zjištění při vyhodnocování	správce IS nebo vedoucí oddělení aplikací a databází	Kap. 9.2	V případě identifikovaných nedostatků při vyhodnocení
schvalování opatření na základě zjištění při vyhodnocování	vedoucí odboru informatiky KÚPK	Kap. 9.2	V případě identifikovaných nedostatků při vyhodnocení
schválení zápisu z vyhodnocení	vedoucí odboru informatiky KÚPK	Kap. 9.2	Podle potřeby

Tabulka č. 17: Odpovědnosti za jednotlivé oblasti Informační koncepce.

10.2 Splnění zákonných povinností

Odpovědnost za splnění zákonných povinností byla stanovena na ředitele Krajského úřadu Plzeňského kraje.

Dílčí odpovědnosti za splnění konkrétních zákonných povinností jsou uvedeny v následující tabulce.

Povinnost	Oblast	Odpovědnost
Zák. č. 365/2000 Sb. §4 odst. 1 písm. a	spolupracovat s MV při vyhledávání, zpracovávání, ukládání a vytváření nových informací, které jsou znalostní základnou pro kvalitní vytváření a rozvoj informačních systémů veřejné správy	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §4 odst. 1 písm. b	spolupracovat s MV při zpracovávání návrhů strategických dokumentů v oblasti informačních systémů veřejné správy, a to i z hlediska bezpečnosti těchto systémů, a předkládání těchto dokumentů vládě, sledování a analýza informační potřeby veřejné správy a stavu informačních systémů veřejné správy	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §4 odst. 1 písm. c	spolupracovat s MV na přípravě nebo koordinaci přípravy záměrů pro budování nebo přetváření informačních systémů veřejné správy spravovaných státními orgány nebo informačních systémů veřejné správy spravovaných orgány územních samosprávných celků, které slouží výlučně k výkonu přenesené působnosti, vyvolané společnou potřebou více správců informačních systémů veřejné správy	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §4 odst. 1 písm. d	spolupracovat s MV na přípravě nebo koordinaci přípravy záměrů pro budování nebo přetváření informačních systémů veřejné správy spravovaných státními orgány nebo informačních systémů veřejné správy spravovaných orgány územních samosprávných celků, které slouží výlučně k výkonu přenesené působnosti, vyvolané potřebou spolupráce a koordinace na mezinárodní úrovni	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §4 odst. 1 písm. e	spolupracovat s MV při vyjadřování se k návrhům dokumentací programů obsahujících pořízení nebo technické zhodnocení určených informačních systémů vypracovaných podle zvláštního právního předpisu. Ministerstvo přitom přihlíží zejména k oprávněným zájmům předkladatele dokumentace programu a k potřebám zajištění řádného výkonu veřejné správy	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §4 odst. 1 písm. f	spolupracovat s MV při zajištění tvorby metodických pokynů pro výkon odborných činností spojených s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §4 odst. 1 písm. g	spolupracovat s MV při koordinaci a vytváření podmínek pro činnost veřejné správy prostřednictvím veřejně přístupných informačních systémů veřejné správy, včetně dálkového přístupu	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §4 odst. 1 písm. h	spolupracovat s MV při koordinaci a vytváření podmínek pro činnost kontaktních míst veřejné správy.	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §5 odst. 1	provádět výběr technických a programových prostředků a dalších produktů pro provoz jimi vytvářených a spravovaných informačních systémů veřejné správy; to neplatí, předpokládá-li informační koncepce České republiky užití produktu určitých vlastností.	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5 odst. 2 písm. a	spolupracovat s MV ČR při plnění jeho úkolů podle §4 odst. 1, včetně kontroly na místě podle §4 odst. 2 prováděné MV ČR	vedoucí odboru informatiky KÚPK

Povinnost	Oblast	Odpovědnost
zákon č. 365/2000 Sb., o ISVS §5 odst. 2 písm. b	předložit MV ČR k vyjádření návrhy dokumentací programů obsahující pořízení, obnovu a provozování ICT vypracovaných podle zvláštního právního předpisu[2] a investiční záměry akcí pořízení, obnovy a provozování ICT, jejichž registrace v Informačním systému financování reprodukce majetku, zadání jejich realizace a změna jejich závazně stanovených parametrů se provádí pouze se souhlasem Ministerstva financí podle zvláštního právního předpisu[3]. Náležitosti dokumentací programů a investičních záměrů stanoví zvláštní právní předpis[3]	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5 odst. 2 písm. c	předložit MV před zahájením poskytování ISVS jimi spravovaným určeným informačním systémem nebo na žádost MV provozní dokumentaci určeného IS k posouzení, zda určený IS splňuje požadavky kladené na něj právními předpisy upravujícími informační nebo komunikační technologie, informační koncepcí orgánu veřejné správy a provozní dokumentací, a jde-li o ISVS spravovaný orgánem veřejné správy, pro něhož jsou závazná usnesení vlády, rovněž informační koncepcí České republiky a jinými usneseními vlády týkajícími se informačních nebo komunikačních technologií	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5 odst. 2 písm. d	zajistit, aby vazby jimi provozovaného informačního systému na informační systémy jiného provozovatele byly uskutečňovány prostřednictvím referenčního rozhraní s využitím datových prvků vyhlášených ministerstvem a vedených v informačním systému o datových prvcích	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5 odst. 2 písm. e	odstranit zjištěné nedostatky ve lhůtě stanovené MVČR	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5 odst. 2 písm. f	předložit MV k vyjádření a v případě určených informačních systémů spravovaných orgány územních samosprávných celků, které slouží výlučně k výkonu samostatné působnosti, na vědomí projekty určených informačních systémů	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5 odst. 2 písm. g	uskutečnit programy obsahující pořízení nebo technické zhodnocení určených informačních systémů, jejichž návrhy dokumentace jsou povinny předložit MV k vyjádření, investiční záměry akcí pořízení nebo technického zhodnocení určených informačních systémů, které jsou povinny předložit MV k vyjádření, a projekty určených informačních systémů, které jsou povinny předložit MV k vyjádření, až po souhlasném vyjádření ministerstva nebo souhlasném rozhodnutí vlády	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §5 odst. 2 písm. h[4]	provádět hodnocení ekonomické výhodnosti způsobu provozu jimi spravovaných informačních systémů veřejné správy,	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §5 odst. 2 písm. i[5]	provádět před pořízením informačního systému veřejné správy nebo v rámci technického zhodnocení anebo rozvoje jimi spravovaného informačního systému veřejné správy hodnocení ekonomické výhodnosti jeho provozu.	vedoucí odboru informatiky KÚPK

[2] Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů.

[3] Vyhláška č. 231/2005 Sb., o účasti státního rozpočtu na financování programů pořízení a reprodukce majetku, ve znění vyhlášky č. 269/2005 Sb.

[4] Ustanovení platné do 31.1.2022

[5] Ustanovení platné do 31.1.2022

Povinnost	Oblast	Odpovědnost
Zák. č. 365/2000 Sb. §5 odst. 2 písm. h[6]	oznámit ministerstvu zahájení zkušebního provozu určeného informačního systému souvisejícího s jeho pořízením nebo technickým zhodnocením před tím, než tato skutečnost nastane, vést záznam o průběhu zkušebního provozu a zpřístupnit záznam ministerstvu dálkovým přístupem; část věty před středníkem se nepoužije v případě zkušebního provozu souvisejícího s technickým zhodnocením určeného informačního systému spočívajícím jen ve změnách nemajících vliv na vnitřní vazby tohoto určeného informačního systému nebo na vazby na jiné informační systémy veřejné správy,	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §5 odst. 2 písm. i[7]	zahájit poskytování služby informačního systému veřejné správy jím spravovaným určeným informačním systémem až po vyjádření ministerstva, že určený informační systém splňuje požadavky kladené na něj právními předpisy, informační koncepcí orgánu veřejné správy a provozní dokumentací, a jde-li o informační systém veřejné správy spravovaný orgánem veřejné správy, pro něhož jsou závazná usnesení vlády, rovněž informační koncepcí České republiky a jinými usneseními vlády týkajícími se informačních systémů veřejné správy; část věty před středníkem se nepoužije na službu informačního systému veřejné správy, která se týká výlučně výkonu samostatné působnosti,	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §5 odst. 2 písm. j[8]	provádět hodnocení ekonomické výhodnosti způsobu provozu jimi spravovaných informačních systémů veřejné správy	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §5 odst. 2 písm. k[9]	provádět před pořízením informačního systému veřejné správy nebo v rámci technického zhodnocení anebo rozvoje jimi spravovaného informačního systému veřejné správy hodnocení ekonomické výhodnosti jeho provozu	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5a odst. 2	vytvářet a vydávat Informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5a odst. 3	vytvářet a vydávat provozní dokumentaci k jednotlivým ISVS, uplatňovat ji v praxi a vyhodnocovat její dodržování	vedoucí odboru informatiky KÚPK
zákon č. 365/2000 Sb., o ISVS §5a odst. 4	zajistit atest dlouhodobého řízení ISVS	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §5b odst. 1	uplatňovat opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.	vedoucí odboru informatiky KÚPK
Zák. č. 365/2000 Sb. §5b odst. 2	při využívání cloud computingu postupovat podle bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu podle právního předpisu upravujícího kybernetickou bezpečnost.	vedoucí odboru informatiky KÚPK

Tabulka č. 18: Odpovědnosti za splnění konkrétních zákonných povinností.

[6] Ustanovení platné od 1.2.2022

[7] Ustanovení platné od 1.2.2022

[8] Ustanovení platné od 1.2.2022

[9] Ustanovení platné od 1.2.2022

11 Implementace cílů, principů a zásad Informační koncepce ČR

11.1 Implementace cílů IK ČR

Název cíle IK ČR	Implementace
01 - UŽIVATELSKY PŘÍVĚTIVÉ A EFEKTIVNÍ „ON-LINE“ SLUŽBY PRO OBČANY A FIRMY	
1.1: Katalog služeb veřejné správy	Přehled služeb je dostupný na webu kraje dle působností jednotlivých útvarů. Pro vymezení životních situací je využíván katalog Portálu veřejné správy v aktuální podobě. *Plánovaná činnost: Provést analýzu vhodného řešení oblasti katalogu služeb a životních situací kraje s ohledem na centrální katalogy a udržitelnost informací v aktuální podobě. (ředitel KUPK, 31.12.2023)*
1.2: Informování o službách veřejnosti	Portál služeb – publikace centrální místo informování veřejnosti a telefonního kontaktu na webu – existence centrálního telefonní uzlu
1.3: Rozvoj univerzálních front-office služeb	Poskytování samoobslužných kanálů pro e-podání (přes datové schránky)
1.4: Rozvoj klientských služeb resortů	KUPK publikuje služby, dle oprávnění typu subjektu, dále jsou Portál ZZO se službami pro tyto organizace.
1.5: Rozvoj Národního katalogu otevřených dat	KUPK doplňuje datové sady ze svých informačních systémů do Národního katalogu otevřených dat. U nových systémů je součástí požadavků využití těchto datových sad.
1.6: Stanovení rolí a zodpovědnosti za služby OVM	Definovány role a odpovědnosti v rámci IK, systému řízení bezpečnosti.
1.7: Systém zapojení veřejnosti a subjektů do zlepšování EG služeb	Definovat proces sběru podnětů veřejnosti a jejich vyřizování, Na web implementovat formulář pro sběr podnětů veřejnosti / na webu dostupný dotazník šetření spokojenosti (vč. námětů na zlepšení), dále se provádějí kampaně při tvorbě strategických dokumentů. Směrem dovnitř úřadu existuje definovaný proces sběru, vyhodnocení a realizace inovačních námětů; vstupní místem pro sběr námětů je rovněž HelpDesk. *Plánovaná činnost: Analýza možnost pro sběr zpětné vazby občanů i zaměstnanců (ředitel KUPK, 31.12.2022)*
1.8: Metodiky a principy uživatelské přívětivosti	V požadavcích ZD je obsažen požadavek na analýzu a návrh z pohledu uživatelské přívětivosti
02 - DIGITÁLNĚ PŘÍVĚTIVÁ LEGISLATIVA	
2.1: Zajistit povinnost vytváření digitálně přívětivé legislativy	Není relevantní

Název cíle IK ČR	Implementace
2.2: Podíl na tvorbě evropské legislativy	Není relevantní
2.3: Projekty eSbírka a eLegislativa	Není relevantní
2.4: Analyzování a úpravy právních předpisů pro služby EG	Právní odbor průběžně provede analýzu legislativy, následně řeší v součinnosti s věcnými útvary a IT
2.5: Zakotvení práva na digitální služby	KUPK přikročí k implementaci zákona
2.6: Aktualizace legislativy k eGovernmentu	Není relevantní
2.7: Analýza služeb EG směrem ke komerčnímu sektoru a klientům	Není relevantní
2.8: Metodika pro veřejné zakázky v ICT a EG	Není relevantní
2.9: Nové návrhy právních předpisů na podporu eGovernment	Není relevantní
03 - ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	
3.1: Využití prostředků ESF na rozvoj digitalizace	Není relevantní
3.2: Digitalizace dosud nedigitalizovaného obsahu	KUPK provedlo analýzu a vyhodnocení efektivity; digitalizace proběhla v rozsahu dle potřeb úřadu.
3.3: Digitalizace a správa úředních dokumentů a úředního obsah	Zajištěno v prostředí spisové služby.
3.4: Zkvalitnění Registru práv a povinností a jeho obsahu	Agendy RPP pro KUPK odpovídají výkonu KUPK.
3.5: Rozvoj komunikační infrastruktury státu	KUPK využívá datových a hlasových služeb Komunikační infrastruktury veřejné správy / CMS.
3.6: Rozvoj systémů elektronické identifikace (EID)	Využíváno prostřednictvím portálu občana, další dle rozvoje dílčích systémů.
3.7: Prostorová data	Digitální technická mapa kraje, Výdej geodat a dat ÚAP, publikování mapových služeb, povodňové systémy – sdílení dat realizováno bez omezení přístupů primárně prostřednictvím Geoportálu
3.8: Kybernetická bezpečnost	Naplňování požadavků dle ZoKB, kraj se podílí na vzdělání ZZO

Název cíle IK ČR	Implementace
04 - ZVÝŠENÍ KAPACIT A KOMPETENCÍ ZAMĚSTNANCŮ VE VEŘEJNÉ SPRÁVĚ	
4.1: Úpravy systemizace a katalogizace profesí v IT a DPL	KUPK používá systemizaci, provede vyhodnocení a případně návrhy úprav profesí.
4.2: Opatření pro získání a udržení klíčových specialistů v rámci veřejné správy	Provést analýzu možnost pro zlepšení situace pro získání, udržení a rozvoj klíčových specialistů v oblasti IT (vedoucí personálního oddělení 31.12.2022)
4.3: Intenzivní spolupráce s vysokými školami	Probíhají spolupráce s regionálními vysokými školami i příjmy a adaptace absolventů a péče o ně
4.4: Sdílená kompetenční centra a zvyšování kapacit	Vytvoření sdílených rolí pro ZO (zejm. prostřednictvím Střediska služeb školám), příp. poskytováno i dalším subjektům.
4.5: Institucionalizace klíčových útvarů a rolí v úřadech	Existence směrnice projektového řízení KUPK *Plánovaná činnost: Analýza možností vytvoření projektové a architektonické kanceláře a vzniku metodiky Enterprise architektury (ředitel KUPK, 31.12.2022)*
4.6: Kompetence a zdroje pro realizaci změn	V rámci předpisů jsou oblasti změn řešeny – specifická směrnice pro change management v současnosti neexistuje *Plánovaná činnost: Analýza potřeb a využití, případně požadavky na směrnici change managementu sumarizovat do specifické směrnice (vedoucí odboru informatiky, 31.12.2022)*
4.7: Zavedení procesního řízení a řízení služeb ve veřejné správě	Zavedeny role manažer kvality, částečně zaveden systém procesního řízení, *Plánovaná činnost: Provést analýzu možností implementace procesního řízení na celý úřad ve spojitosti s implementací Metodického pokynu MVČR pro řízení kvality ve služebních úřadech (ředitel KUPK, 30.6.2022)*
4.8: Rozvoj systému vzdělávání a odborné přípravy zaměstnanců veřejné správy směrem k EG	Řešeno v rámci standardního procesu vstupního, průběžného vzdělávání rolí – využívány i e-kurzy
05 - EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	
5.1: Implementace procesu řízení IKČR	Není relevantní
5.2: Alokace lidských a institucionálních zdrojů pro realizaci IKČR	Není relevantní
5.3: Zavedení principů pro řízení a rozvoj architektury v úřadech	Zavedení principů a postupů „Enterprise architektury“ – viz výše

Název cíle IK ČR	Implementace
5.4: Realizace modelu spolupráce OVM a podniků poskytujících infrastrukturu	Rozvoj korporátních služeb
5.5: eGovernment cloud	V současném stavu není eGovernment cloud, vzhledem ke stavu jeho přípravy využíván
5.6: Standardizace v EG a službách	Dodávky v oblasti ICT jsou řízeny pomocí SLA
5.7: Podpora agend vykonávaných v přenesené působnosti formou sdílení údajů a AISů	Využívány existující centrální AISy (např. Státní pokladna, Dopravní agendy), KUPK připraveno k připojení na další dle jejich vzniku.
5.8: Podpora agendových systémů pro výkon samostatné působnosti	KUPK pro svou samosprávnou působnost buduje informační systémy, které poskytují své digitální služby všemi dostupnými kanály, případně AIS, a to vč. sdílení pro ZZO.
5.9: Rozvoj Propojeného datového fondu (PPDF)	KUPK napojen na Základní registry, CMS, využití centrálních systémů, pokud jsou k dispozici.
5.10: Rozvoj otevřených dat a veřejného fondu dat a služeb veřejné správ	KUPK vyžívá Národní katalog otevřených dat, viz 1.5: Rozvoj Národního katalogu otevřených dat
5.11: Rozvoj geoinformatiky a prostorových informací	Digitální technická mapa kraje, Výdej geodat a dat ÚAP, publikování mapových služeb, povodňové systémy – sdílení dat realizováno bez omezení přístupů primárně prostřednictvím Geoportálu
5.12: Hodnocení realizace IKČR a zpětná vazba	KUPK poskytne součinnost pro celostátní koordinaci IKČR, v průběhu roku 2022 vyhodnotíme míru implementace IKČR KUPK
5.13: IS nové generace	KUPK buduje IS s využíváním automatizace v rámci IS – zejm. řízení workflow, podpory procesů apod.
IK06 – EFEKTIVNÍ A PRUŽNÝ DIGITÁLNÍ ÚŘAD	
6.1: Podpora práce úředníků	Podporováno vnitřními funkcionalitami provozních a podpůrných systémů KUPK.
6.2: Vnitřní elektronizace	Provedena digitalizace v mnoha oblastech, zejm. spisová služba a vnitřní procesy; dále probíhá rozvoj v oblasti digitalizace.
6.3: Nové metody řízení úřadu	KUPK má zaveden systém řízení služeb, rovněž částečně i procesní řízení – viz cíl 4.7
6.4: Nové provozní a podpůrné systémy	Probíhá standardně
6.5: Vnitřní infrastruktura	KUPK aktuálně disponuje kvalitní infrastrukturou; modernizace probíhá průběžně, rozvoj infrastruktury dále plánován

Tabulka č. 19: Implementace cílů IK ČR

11.2 Implementace principů IK ČR

Název principu IK ČR	Implementace
P 1: Standardně digitalizované (Digital by default)	KUPK poskytuje digitální služby se vstupy elektronickým podáním prostřednictvím datových schránek
P 2: Zásada „pouze jednou“ (Once only)	Využíván datový sklad (i pro ZZO). KUPK využívá data ze Základních registrů, dále obecně využívá datové sady centrální úřadů.
P 3: Podpora začlenění a přístupnost (Inclusiveness and Accessibility)	Zajištěn soulad s vyhláškou č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti)
P 4: Otevřenost a transparentnost (Openness and Transparency)	Zajištěno povinné zveřejňovaní informací podle vyhlášky č. 442/2006, která stanoví strukturu informací zveřejňovaných o povinném subjektu dle § 5 odst. 1 a 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
P 5: Přeshraniční přístup jako standard (Crossborder interoperability)	Dostupnost elektronických služeb není omezena geograficky.
P 6: Interoperabilita jako standard (Interoperability by design)	IS KUPK mají definována API pro vzájemnou komunikaci, pro předávání dat uvnitř úřadu slouží rovněž datový sklad KUPK.
P 7: Důvěryhodnost a bezpečnost (Security & Privacy by design)	Při ochraně osobních údajů se zaměstnanci KUPK řídí Nařízením Evropského parlamentu a Rady (EU) 2016/679, ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
P 8: Jeden stát (Whole-of-Government)	KUPK vyžívá centrálních systémů (CMS – dopravní agendy, Státní pokladna, …), mezikrajsky funguje videokonferenční systém, pro ZZO a obce poskytuje sdílené služby.
P 9: Sdílené služby veřejné správy (Shared Services)	KUPK využívá existující služby CMS, NIA, Základní registry; připravenost využít dalších centrálních sdílených služeb v závislosti na jejich dostupnosti.
P 10: Připravenost na změny (Flexibility)	Zavedeny procesy rozvoje informačních systémů.
P 11: eGovernment jako platforma (Embedded eGovernment)	Analytické práce nad záměrem pořízení nového ISVS nebo změny ISVS obsahují i vymezení procesů, které bude IS zajišťovat či podporovat; legislativní upgrady ošetřeny ve smlouvách s dodavateli, zajištěna detailní technická dokumentace
P 12: Vnitřně pouze digitální (Inside only digital)	Existující podpora agend i provozních procesů IS (dokumentace, docházka, úkoly, spisová evidence apod.)

Název principu IK ČR	Implementace
P 13: Otevřená data jako standard (Open Data by default)	Data, která jsou žádána a mohou být publikována, jsou přístupná na webu. KUPK reaguje na poptávku třetích stran, případně dostupná data rozšiřuje.
P 14: Technologická neutralita (Technological neutrality)	Využívání webových služeb
P 15: Uživatelská přívětivost (User-friendliness)	Uživatelská přívětivost je součástí zadání a testování IS při akceptačním řízení
P 16: Konsolidace a propojování informačních systémů veřejné správy (IT Consolidation)	Hledání synergických efektů a koordinace s rozvojem informačních systémů stávajících je prováděno v rámci analytických prací v rámci přípravy pořízení / změn IS
P 17: Omezení budování monolitických systémů (Application decomposition)	KUPK použije modulární přístup k řešení agend při obnově stávajících systémů

Tabulka č. 20: Implementace principů IK ČR

11.3 Implementace zásad IK ČR

Název zásad IK ČR	Implementace
Z 1: Na prvním místě je klient	Vymezení procesů, které má IS částečně či úplně zajišťovat či podporovat je prováděno v rámci analytických prací v rámci přípravy pořízení / změn IS
Z 2: Standardy plánování a řízení ICT	IT řízeno na základě principů norem ISO 20000 a ISO 27001. Částečně zaveden systém ISO 9001.
Z 3: Strategické řízení pomocí IK OVS	Oblast IT je řízena tímto dokumentem – informační koncepcí na základě vymezení Informační strategie
Z 4: Řízení architektury	Model Enterprise architektury KUPK – vytvořen v .archi
Z 5: Řízení požadavků a změn	Zavedení change managementu (PM)
Z 6: Řízení výkonnosti a kvality	Jsou definovány cíle kvality (viz kapitola 7), u poskytování služeb definovány SLA.

Název zásad IK ČR	Implementace
Z 7: Řízení zodpovědnosti za služby a systémy	Definovány a určeny role věcného i technického správce pro všechny IS KUPK, určen i provozovatel (viz příloha č.2).
Z 8: Řízení katalogu služeb	Existuje katalog ICT služeb
Z 9: Udržení interních kompetencí	Systém mentoringu v rámci celého úřadu, systém porad, dokumentací systémů, GA, DNI, dokumentace skutečného provedení atp., fungující vzdělávání (v oblasti IS garantem).
Z 10: Procesní řízení	Částečně zaveden systém řízení kvality (ISO 9001), definovány postupy v IT (viz kapitola 9, 10, 11).
Z 11: Řízení přínosů a hodnoty	Záměr pořízení IS (jako podklad pro rozhodování o pořízení systému) obsahuje zdůvodnění, včetně popisu přínosů pro veřejnost/zaměstnance a KUPK – viz kapitola 9.2.2.
Z 12: Řízení kapacit zdrojů	Dlouhodobé řízení kapacit probíhá formou systemizace pracovních a služebních míst. Součástí záměru pořízení IS je vymezení potřebných zdrojů (vč. lidských), které je třeba na fáze pořízení i zajištění provozu zajistit. Alokovat potřebné zdroje k zajištění IT (věcní správci a další na projekty a rozvoj).
Z 13: Nezávislost návrhu, řízení a kontroly kvality	Pořízení a významné změny IS budou řízeny jako projekty. Vedoucím projektu je věcný správce, případně jiný určený pracovník dle metodiky projektového řízení. Fungující IA, procesy kontroly dodavatelů.
Z 14: Vztah informatiky a legislativy	KUPK nemá kompetence v oblasti definice legislativy na národní úrovni. Při definici pravidel finančních zdrojů spravovaných KUPK je brán ohled na zajištění procesů (zejména komunikace) prostřednictvím elektronických (IT) nástrojů.
Z 15: Řízení financování ICT	Financování ICT je funkční – viz kap. 8
Z 16: Využívání otevřeného software a standardů	Otevřený SW může být využíván v případě, kdy nejsou kladeny žádné požadavky na kvalitu systému (z pohledu SLA parametrů) ani požadavky bezpečnostní (ZoKB, GDPR, apod).
Z 17: Podpora vyváženého partnerství s dodavateli	S ohledem na ekonomickou výhodnost a finanční možnosti KUPK nepořizuje standardně IS vč. licence k užití zdrojových kódů (nevýhradní).

Tabulka č. 21: Implementace zásad IK ČR

12 Přílohy

Součástí Informační koncepce jsou následující přílohy (vždy ve verzi, která je shodná s verzí Informační koncepce):

1. **Seznam významných IS spravovaných nebo provozovaných KÚPK**
2. **Charakteristiky ISVS a vybraných PIS spravovaných nebo provozovaných KÚPK**

13 Seznam tabulek a obrázků