Karlovarský kraj

Informační koncepce
dle zákona č. 365/2000 Sb., o ISVS, ve znění pozdějších předpisů

2013-2018

Sledování dokumentu

Rozdělovník

JMÉNO	ORGANIZACE	PŘEDÁNO (dne)	Č. VÝTISKU
Karel Kolařík	KUKK		
Mgr.Daniel Tovth	KUKK		
Archiv			

Verze	VYPRACOVAL	PŘEDMĚT	DATUM
1.0	BE-MI. CZ s.r.o.	Nový dokument	25.10.2013
1.1	Ing. Petr Kulda	Aktualizace dokumentu	28.3.2017

Obsah

Seznam tabulek

Seznam zkratek a pojmů

Atest DŘ ISVS – Atest dlouhodobého řízení ISVS

BPIS KK – Bezpečnostní politika krajského úřadu Karlovarského kraje

ICT – Informační a komunikační technika

IK – Informační koncepce ISVS

IS – Informační systémy

ISMS - Systém řízení bezpečnost informací (Information Security Management System)

ISVS – Informační systémy veřejné správy

ISZR – Informační systém základních registrů (správce MV, provozovatel Správa ZR)

KK – Karlovarský kraj

MVČR – Ministerstvo vnitra

N/A – Informace není k dispozici

OPI – Odbor projektového řízení a informatiky KK

OVS – Orgán veřejné správy

PIS – Provozní informační systémy veřejné správy

SLA - Smlouva o technické podpoře

SBPIS KK – Systémová bezpečnostní politika informačního systému Karlovarského kraje

[1] **Zákon č. 365/2000 Sb., o ISVS** – zákon č. 365/2000 Sb., o informačních systémech veřejné správy ve znění pozdějších předpisů

[2] **Vyhláška č. 529/2006 Sb.,** o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy

Správce ISVS - viz [1], §2, písm. c: správcem ISVS je subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá

Správce aplikace – správce (administrátor) dané aplikace, ISVS.

1 Souhrnná část Informační koncepce

1.1 Identifikační údaje

Organizace	
Název organizace	Karlovarský kraj
Typ organizace	Vyšší územně samosprávní celek
IČ	70891168
Adresa	Závodní 353/88, 360 06, Karlovy Vary
Telefon:	354 222 300 (ústředna)
Fax:	353 331 509 (podatelna)
E-mail:	epodatelna@kr-karlovarsky.cz
Web:	http://www.kr-karlovarsky.cz
ID Datové schránky	siqbxt2
Informační koncepce	
Aktuální verze	1.1
Doba platnosti	5 let
Schvalovatel	vedoucí odboru projektového řízení a informatiky KK

Tabulka 1-1 Identifikační údaje

1.2 Aktuální verze Informační koncepce

Aktuální verze IK		
Verze	v 1.1	
Datum vydání	28.3.2017	
Datum schválení	14.4.2017	
Datum platnosti od:	14.4.2017	
Vytvořil/útvar, společnost:	Odbor projektového řízení a informatiky KK	
Schválil/,jméno –funkce	Ing. Petr Kulda - Vedoucí odboru projektového řízení a informatiky KK	
Podpis zástupce KK		
Název souboru/umístění souboru	IK_KK_2013_v_1.1/úložiště dokumentace OPŘI	
Počet stran	57	

Tabulka 1-2 Identifikace verze 1.0 Informační koncepce

1.3 Předchozí verze Informační koncepce

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 zásadních změnách v oblasti ISVS KK, případně na základě odborných auditů a studií.

Změny ve verzi IK:			
Verze	**Popis změny**	**Důvod**	**Místo (v dokumentu)**
1.0	Byla zpracována informační koncepce Verze 1.0. Tato nová informační koncepce nahrazuje předchozí IK vydanou dne 20.12.2009	Požadavek zákona č.365/2000 Sb., o ISVS	Nový dokument

Tabulka 1-3 Změny ve verzi IK

2 Zdroje a východiska

2.1 Právní podklad tohoto dokumentu

Základním právním předpisem zavádějící pojem Informační koncepce je zákon č. 365/2000 Sb., o ISVS, ve znění pozdějších předpisů. Konkrétně § 5a, zákona definuje požadavek pro orgány veřejné správy vytvořit a vydat Informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování. V Informační koncepci orgány veřejné správy stanoví své dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných informačních systémů veřejné správy a vymezí obecné principy pořizování, vytváření a provozování informačních systémů veřejné správy.

Strukturu a obsah dokumentu IK upřesňuje prováděcí vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah Informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy.

2.2 Legislativní rámec

Legislativní rámec k ISVS představují kromě zákona č. 365/2000 Sb., o ISVS, jeho prováděcí vyhlášky. Doplňujícím „výkladem“ zákona jsou pak metodické pokyny.

- Zákon č. 365/2000 Sb., o ISVS, ve znění pozdějších předpisů
- Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy
- Vyhláška č. 53/2007 Sb., o referenčním rozhraní
- 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. 528/2006 Sb., o informačním systému o informačních systémech veřejné správy
- Vyhláška č. 469/2006 Sb., o informačním systému o datových prvcích
- 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

2.3 Související dokumentace

- Informační koncepce v.1.1 ze dne 20.12.2009

- č. SE 01/2006 Bezpečnostní politika informačního systému krajského úřadu Karlovarského kraje
- Metodika řízení projektů
- Strategie Karlovarského kraje pro oblast Governmentu Krajský úřad Karlovarského kraje, odbor informatiky.
- Studie proveditelnosti.
- Archivace elektronické (emailové) pošty- popis projektového záměru
- Návrh provozních a bezpečnostních pravidel Regionální komunikační infrastruktury (RKI) - popis projektového záměru
- Rozvoj technologického centra (TCK) - popis projektového záměru
- Upgrade existující LAN infrastruktury KUKK - popis projektového záměru

3 Informační systémy ve správě KK

V této části IK je uveden přehled jednotlivých informačních systémů KK. Informační systémy jsou v IK rozděleny dle zákona č. 365/2000 Sb., o ISVS na:

- Informační systém veřejné správy (ISVS)
- Provozní informační systémy (PIS) s vazbou na ISVS
- Informační systémy provozované pro příspěvkové organizace KK

Doplňujícím dělení je vyznačení významných informačních systémů dle Zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Takové systému mají v názvu uvedenu zkratku VIS (významný informační systém). Každý VIS je současně ISVS.

3.1 Informační systémy veřejné správy a významné informační systémy KK

V následujícím textu jsou popsány ISVS KK.

3.1.1 AthenA – Spisová služba - VIS

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	KK
Dodavatel	Pilscom s.r.o.	**Garant IS**	Bc. Smaržík
Pořizovací náklady	493 tis Kč	**Roční provozní náklady**	237 tis Kč
Napojení na ISZR	Ano	**Registrovaná Agenda**	A1343
Spravující právní předpis	Zákon č. 499/2004 Sb., o archivnictví a spisové službě		
Typ dostupné dokumentace IS	Příručka administrátora Uživatelská příručka + online nápověda		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ano		
Vazba na ISVS jiného správce	MVCR - IS DATOVÝCH SCHRÁNEK, CZECHPOINT		
Vazby (interní)	Stavební úřad, elektronická podatelna		
Technické a programové prostředky	Client – server, platforma MS Windows, databáze SQL, DOtNET		
Charakteristika			
Páteřní informační systém pro řízení spisové dokumentace úřadu - kompletní správa, evidence veškerých údajů o dokumentech i spisech včetně sledování jejich pohybu v organizaci po celý jejich životní cyklus. Propojení na jiné interní a externí informační systémy např. ISDS, CZECHPOINT apod.			

3.1.2 Integrační sběrnice - VIS

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	TESCO SW a.s.	**Garant IS**	Bc. Smaržík
Pořizovací náklady	15.400 tis. Kč	**Roční provozní náklady**	655 tis. Kč
Napojení na ISZR	Ano	**Registrovaná Agenda**	Všechny ohlášené KK
Spravující právní předpis	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, č. 111/2009 Sb., o základních registrech		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ano		
Vazba na ISVS jiného správce	JIP, ISZR		
Vazby	Spisová služba, PaM, Ekonomický systém, Stavební úřad, Portál úředníka, IDM		
Technické a programové prostředky	Platforma MS Windows, Linux, MS BizTalk, SilverLight, .net, Novell eDirectory, DB MS SQL		

Charakteristika

Integrační platforma Enterprise Service Bus zprostředkovává a řídí komunikaci lokálních AIS s ISZR. Zajišťuje logování dotazů odesílaných na ISZR dle požadavků zákona.

Integrace s vnějšími IS

- Integrace s centrálními registry
- Integrace se službami eGON
- Integrace se službami CMS
- Identity management

3.1.3 GINIS - VIS

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Gordic, spol. s r.o.	**Garant IS**	Bc. Kořínek

Pořizovací náklady	2 008 tis Kč	**Roční provozní náklady**	568 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 563/1991 Sb., o účetnictví Zákon č. 586/1992 Sb., o daních z příjmů		
Typ dostupné dokumentace IS	Dílčí elektronické příručky		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ano		
Vazba na ISVS jiného správce	Elektronické bankovnictví, IIS Státní pokladny		
Vazby (interní)	Ne		
Technické a programové prostředky	Client – server, platforma Windows, DB MS SQL, .net		
Charakteristika			
IS slouží k zajištění ekonomických agend			

3.1.4 Webový portál - VIS

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	KK
Dodavatel	Ne	**Garant IS**	M.Dohnalová
Pořizovací náklady	N/A	**Roční provozní náklady**	N/A
Napojení na ISZR	Není	**Agenda**	Úřední deska
Spravující právní předpis	Zákon 500/2004 Sb., správní řád		
Typ dostupné dokumentace IS	Elektronická uživatelská příručka, Technická dokumentace		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ano		
Vazba na ISVS jiného správce	Ne		
Vazby	Ne		
Technické a programové prostředky	Platforma MS sharepoint, publikační systém		
Charakteristika00			
Webový portál http://www.kr-karlovarsky.cz Funkcionality: úřední deska, aktuality, ankety, RSS, otázky a odpovědi, dokumenty a další.			

3.1.5 Elektronická pošta úřadu

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Autocont a.s.	**Garant IS**	Miloš Tříska
Pořizovací náklady	200 tis. Kč	**Roční provozní náklady**	40 tis. Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, č. 111/2009 Sb., o základních registrech		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ano		
Vazba na ISVS jiného správce	Ne		
Vazby	IDM		
Technické a programové prostředky	Platforma MS Windows, BSD Unix, Symantec brightmail, Microsoft Exchange		
Charakteristika			
Elektronická pošta úřadu je systém sestávající z více technických prostředků. Zajišťuje příjem, odesílání a uložení aktuálních zpráv elektronické pošty.			

3.1.6 CLIX – Registr oznámení (ROZ)

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI
Dodavatel	BMI System Czech, a.s.	**Garant IS**	Bc. Kořínek
Pořizovací náklady	291 tis Kč	**Roční provozní náklady**	12 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 159/2006., o střetu zájmů		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		

Vazba na ISVS jiného správce	Ne
Vazby	Ne
Technické a programové prostředky	Webový prohlížeč, MS SharePoint Services, databáze MS SQL Express
Charakteristika	
Evidence oznámení podaných veřejnými funkcionáři, publikace oznámení na internetu, evidence žadatelů o přístup k registru, evidence přístupu k oznámením.	

3.1.7 Digitální mapa veřejné správy

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Vars Brno a.s., NESS Czech s.r.o.	**Garant IS**	Ing. Heliks
Pořizovací náklady	33.000 tis Kč	**Roční provozní náklady**	2.004 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 129/2000 Sb., o krajích, č. 344/1992 sb., o katastru nemovitostí ČR, č. 183/2006., o územním plánování a stavebním, č. 200/1994 sb., o zeměměřičství, č.111/2009 Sb., o základních registrech, Vyhláška č. 26/2007Sb.,		
Typ dostupné dokumentace IS	Dílčí elektronické příručky		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ano		
Vazba na ISVS jiného správce	INSPIRE (Cenia.CZ)		
Vazby	Propojení na Datový sklad KK		
Technické a programové prostředky	Client–server, platforma MS Windows, databáze SQL, DOtNET, SilverRight, Java, Flash, webové služby		
Charakteristika			
Informační systém poskytuje následující služby: územní prvky z registru územní identifikace adres a nemovitostí, digitální katastrální mapa státní mapové dílo Digitálně technické mapy obcí, Základní báze geografických dat ZABAGED, databáze geografických jmen GEONAMES Lokální data územního plánovaní, Data základních registrů, data krajských registrů GIS, data datového skladu KK			

3.1.8 Elektronická podatelna (EPD)

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Pilscom s.r.o.	**Garant IS**	Bc. Smaržík
Pořizovací náklady	50 tis Kč	**Roční provozní náklady**	N/A
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 2272000 Sb., o elektronickém podpisu, nařízení vlády č.304/2001 Sb.		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ano		
Vazba na ISVS jiného správce	Ne		
Vazby (interní)	Spisová služba		
Technické a programové prostředky	Platforma MS Windows, MS Access, MS Outlook, Hostované řešení u společnosti Pilscom s.r.o.		
Charakteristika			
Aplikace pro zajištění provozu elektronické podatelny s využitím kvalifikovaných certifikátů.			

3.1.9 ESPI – Evidence správních řízení

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Inisoft s.r.o.	**Garant IS**	Bc. Buček
Pořizovací náklady	11 tis Kč	**Roční provozní náklady**	41 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	Ne
Spravující právní předpis	Zákon č. 500/2004 Sb., správní řád		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		

Vazba na ISVS jiného správce	Ne
Vazby (interní)	Ne
Technické a programové prostředky	Platforma Windows, DB FireBird
Charakteristika	
Evidence správních řízení v oblasti životního prostředí	

3.1.10 EVI – Evidence odpadů, zařízení

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Inisoft s.r.o.	**Garant IS**	Bc. Buček
Pořizovací náklady	11 tis. Kč	**Roční provozní náklady**	41 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č.185/2001 Sb., o odpadech; vyhláška č . 381/2001 Sb., vyhláška č.383/2001 Sb.,		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		
Vazba na ISVS jiného správce	Ne		
Vazby (interní)	Ne		
Technické a programové prostředky	Platforma Windows, DB FireBird		
Charakteristika			
Evidence odpadů při každém vzniku, zneškodnění nebo předání odpadu, generování hlášení a statistických výkazů.			

3.1.11 EDA – Evidence dopravních agend

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Yamaco Software	**Garant IS**	Ing. Velechovský

Pořizovací náklady	14 tis Kč	**Roční provozní náklady**	22 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 13/1997 Sb., o pozemních komunikacích, č. 111/1994 Sb., o silniční dopravě, č.361/2000 Sb., o provozu na poz. komunikacích, č.200/1990 Sb., o přestupcích, č. 247/2000 Sb., o získávání a zdokonalování odborné způsobilosti k řízení motorových vozidel.		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		
Vazba na ISVS jiného správce	Centrální registr dopravců MD ČR		
Vazby (interní)	Ne		
Technické a programové prostředky	Platforma Windows, DB FireBird		
Charakteristika			
Komplexní informační systém pro agendy odborů dopravy ve státní správě. Obsahuje údaje o správních řízeních, dopravcích, vozidlech, řidičích, stanicích TK, dopravních přestupcích atd.			

3.1.12 Krajské digitální úložiště

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	ICZ a.s.	**Garant IS**	Ing. Nováček
Pořizovací náklady	23.279 tis. Kč	**Roční provozní náklady**	2.056 tis. Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	Ne
Spravující právní předpis	Zákon č. 499/2004 sb., o archivnictví a spisové službě, č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, Vyhláška č.191/2009 sb., o podrobnostech výkonu spisové služby. Standard OAIS		
Typ dostupné dokumentace IS	Dílčí elektronické příručky		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		

Vazba na ISVS jiného správce	KDS – NDA (národní digitální archiv)
Vazby	Spisové služby KÚ a PO, KDJ
Technické a programové prostředky	Platforma MS Windows, databáze SQL, webové služby, webový prohlížeč. KDS – ICZ DESA DES, KDR – ICZ DESA DER, KDU – ICZ IDU (ALFRESCO)
Charakteristika	
Informační systém skládající se z Krajské digitální spisovny (KDS), krajského digitálního repozitáře (KDR), krajského digitální úložiště (KDU). Poskytuje následující služby a data: Uzavřené písemnosti a spisy (výstupy ze spisových služeb obcí a PO v Karlovarském kraji), dokumenty z oblasti kulturního dědictví regionu, důležitá data a dokumenty pocházející z činnosti informačních systémů orgánů veřejné správy na území kraje.	

3.1.13 MRP – Evidence mysliveckých a rybářských průkazů

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Yamaco Software	**Garant IS**	Bc. Buček
Pořizovací náklady	0	**Roční provozní náklady**	3 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 449/2001 Sb., o myslivosti, č. 99/2004 Sb., o rybářství		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		
Vazba na ISVS jiného správce	Ne		
Vazby (interní)	Ne		
Technické a programové prostředky	Platforma Windows, DB FireBird		
Charakteristika			
IS slouží k evidenci loveckých a rybářských lístků, evidenci průkazů lesní a myslivecké stráže, vodní a rybářské stráže, evidenci průkazů mysliveckých a rybářských hospodářů dále pak umožňuje myslivecké plánování a statistiky.			

3.1.14 Medis Alarm

Základní údaje o informačním systému

Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Medistyl, spol. s r.o.	**Garant IS**	Bc. Buček
Pořizovací náklady	18 tis Kč	**Roční provozní náklady**	12 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 57/1998 Sb., o chemických látkách a chemických přípravcích		
Typ dostupné dokumentace IS	Ne		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		
Vazba na ISVS jiného správce	Ne		
Vazby (interní)	Ne		
Technické a programové prostředky	Webový prohlížeč		
Charakteristika			
IS poskytuje údaje o chemických látkách a jejich zpracovatelích slouží k evidenci subjektů nakládajících s nebezpečnými chemickými látkami, evidenci kontrolních činností zpracování správní agendy a udělování autorizací.			

3.1.15 Ovzduší SQL

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	Kvasar, spol. s r.o.	**Garant IS**	Bc. Buček
Pořizovací náklady	19 tis Kč	**Roční provozní náklady**	18 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 86/2002 Sb., o ochraně ovzduší		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		
Vazba na ISVS jiného správce	Ne		
Vazby (interní)	Ne		

Technické a programové prostředky	Platforma Windows, DB MS SQL
Charakteristika	
IS slouží k evidenci zdrojů znečišťování ovzduší, evidenci poplatníků a poplatků za znečišťování ovzduší.	

3.1.16 Stavební úřad

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	VITA software, s.r.o	**Garant IS**	Bc. Buček
Pořizovací náklady	170 tis Kč	**Roční provozní náklady**	49 tis Kč
Napojení na ISZR	Ano	**Registrovaná Agenda**	A569, A565
Spravující právní předpis	Zákon č. 183/2006 Sb., o územním plánování a stavebním úřadu		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		
Vazba na ISVS jiného správce	IS DS		
Vazby (interní)	Katastr nemovitostí, spisová služba		
Technické a programové prostředky	Client – server, platforma Windows, DB MS SQL		
Charakteristika			
IS slouží k evidenci správních řízení a podporu činnosti obecního stavebního úřadu.			

3.2 Provozní Informační systémy KK

3.2.1 Datový sklad Karlovarského kraje

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	NESS Czech s.r.o.	**Garant IS**	Ing. Heliks
Pořizovací náklady	19.5770 tis. Kč	**Roční provozní náklady**	1.038 tis. Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A

Spravující právní předpis	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, č. 101/2000 Sb., o ochraně osobních údajů, č. 121/2000 Sb., autorský zákon.
Typ dostupné dokumentace IS	Elektronická příručka
Současný stav	Ostrý provoz
Předpokládaná změna IS	Ne
Vazba na ISVS jiného správce	Ne
Vazby	ČSÚ, orgány státní správy, ekonomické systémy PO, KÚ (jako zdroje dat)
Technické a programové prostředky	Client –server, platforma MS Windows, webové služby, MS SharePoint Services, databáze MS SQL
Charakteristika	
Datový sklad KK slouží ke sběru, transformaci, zpracování a výsledné prezentaci dat. Zdrojem dat datového skladu KK jsou jednotlivá datová tržiště. Prezentační vrstvu tvoří manažerský informační systém s nástroji BI.	

3.3 Informační systémy provozované pro organizace KK

3.3.1 E-spis LITE

Základní údaje o informačním systému			
Správce ISVS	KK	**Provozovatel**	OPI KK
Dodavatel	ICZ a.s.	**Garant IS**	Ing. Nováček
Pořizovací náklady	1.197 tis Kč	**Roční provozní náklady**	60 tis Kč
Napojení na ISZR	Ne	**Registrovaná Agenda**	N/A
Spravující právní předpis	Zákon č. 499/2004 sb., o archivnictví a spisové službě, č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, Vyhláška č.191/2009 sb., o podrobnostech výkonu spisové služby.		
Typ dostupné dokumentace IS	Elektronická příručka		
Současný stav	Ostrý provoz		
Předpokládaná změna IS	Ne		
Vazba na ISVS jiného správce	MVCR – IS DS		
Vazby	Krajská digitální spisovna		

Technické a programové prostředky	Platforma MS Windows, databáze SQL, webový prohlížeč

Charakteristika
Elektronická spisová služba příspěvkových organizací Karlovarského kraje a negarantované úložiště dokumentů zajišťuje pro jednotlivé organizace – Příjem a evidence dokumentů, oběh a vyřizování dokumentů, práce s el. dokumenty, ukládání v garantovaném i negarantovaném úložišti dokumentů, archivace a skartace dokumentů Propojení na jiné interní a externí informační systémy např. ISDS,

4 Záměry na pořízení, vytvoření nových ISVS nebo změny stávajících ISVS

Krajský úřad Karlovarského kraje v současnosti plánuje realizovat následující projekty:

1. Implementace časových razítek do ISVS eSS AthenA
2. Pořízení nového řešení ISVS Elektronická podatelna
3. Kontrola zakázek digitální technické mapy
4. Společný výměnný formát digitální technické mapy
5. Změna provozní technologie, struktury a vzhledu ISVS Webový portál kraje
6. Centralizovaný log systém
7. Upgrade integrační sběrnice za účelem implementace Active Directory Server 2016
8. Upgrade elektronické pošty úřadu na verzi Exchange server 2016
9. Upgrade ekonomického systému pro podporu veřejné finanční podpory (dotace)
10. Upgrade ekonomického systému pro elektronický oběh účetních dokladů
11. Datový sklad kraje – vytvoření datové kostky projektů
12. Vytvoření systému pro sběr informací od obcí
13. Pořízení nových licencí ArcGis Desktop
14. Pořízení systému pro evidenci a inventarizaci majetku
15. Systém pro evidenci zápisů a úkolů z porad vedení
16. Zavedení elektronického systému vykazování údajů o sociálních službách.

Ke každému zmíněnému projektu je zpracován projektový záměr, který je uložen u vedoucího OPI.

V případě nového záměru na pořízení informačního systému bude tento záměr konkretizován v rámci dalších verzí této IK.

Každý nový záměr bude obsahovat následující informace (minimální rozsah):

- specifikování potřebnosti nového ISVS,
- způsob zajištění financování nového ISVS:
    - očekávané náklady
    - rozhodnutí o způsobu financování (pořízení nebo vytvoření),
    - časová dostupnost zdrojů,
    - harmonogram předpokládaného čerpání zdrojů.
- specifikování výchozího stavu včetně zvážení možností využití existujících IS nebo jejich částí,
    - stanovení cílového stavu IS,
    - stanovení požadavků na kvalitu,
    - stanovení požadavků na bezpečnost,
- předpokládané dopady zavedení nového IS na procesy a činnost orgánu veřejné správy,

- specifikování druhů dopadu (např. nutná organizační opatření, personální dopady apod.)
- způsob zabezpečení dopadů v celém systému OVS
- předpoklad eliminace nepříznivých dopadů

V případě předpokládaného pořizování IS od dodavatele budou součástí zadání ještě podmínky pro:

- řízení jakosti,
- řízení bezpečnosti,
- projektové řízení u dodavatele, včetně specifikace příslušné normy, podle které bude realizováno,
- pro dodání (dokumentace IS, školení, podrobnosti testování a přejímky),
- způsob a zajištění údržby a změn IS.

Výjimka zde platí pro případ přímého nasazení nového IS od jiného subjektu, kde výše uvedené informace zajišťuje daný subjekt. Po implementaci IS uvede správce IK tento IS v kap. 3 v rámci nové verze IK.

Při práci se záměry projektu je dále postupováno dle Metodiky řízení projektů verze 02 ze dne 27. 8 .2012[1]

[1] Metodika dle PRINCE2

5 Řízení kvality ISVS

V současné době (doba tvorby IK) je oblast kvality KK řízená v rámci zavedené metodiky řízení projektů. Metodika řízení projektů pokrývá oblast kvality přes celý životní cyklus projektu a zahrnuje i oblast ISVS.

Řízení kvality v oblasti informačních systémů sestává z následujících dílčích oblastí:

- Stanovení dlouhodobých cílů
- Stanovení požadavků na kvalitu
- Plánu řízení kvality

5.1 Dlouhodobé cíle v oblasti řízení kvality ISVS

Mandatorní požadavky kodifikované v §3 vyhl. č. 529/2006 Sb., o DŘ ISVS, požadují následující obsah a strukturu dlouhodobých cílů pro oblast ISVS ve správě příslušného orgánu veřejné správy:

- **Zajištění kvality dat, která jsou v těchto systémech zpracovávána,**
- **Zajištění kvality technických a programových prostředků,**
- **Zajištění kvality služeb, které jsou prostřednictvím těchto systémů poskytovány.**

V souvislosti s rozdělením IS ve správě orgánu veřejné správy podle zákona č. 365/2000 Sb., na ISVS a PIS se požadavky na kvalitu u ISVS a PIS neliší - protože v obou případech musí být stejně vysoké, pouze u ISVS budou detailněji dokumentovány pro zajištění potřeby průkaznosti.

Dlouhodobé cíle v oblasti řízení kvality IS:

I. U pořizovaných ISVS a ISVS uváděných do provozu

1. Kvalita procesu implementace ISVS
2. Zajištění požadované kvality technické infrastruktury a robustní softwarové infrastruktury.
3. Zajištění kvality a bezpečnosti zpracovávaných dat.

II. U ISVS v produktivním provozu

1. Zajištění kvality dat zpracovávaných v IS.
2. Zajištění kvality služeb poskytovaných prostřednictvím IS,
3. Zajištění kvality technických a programových prostředků.

5.1.1 Konkrétní cíle kvality u SW projektů nově pořizovaných a uváděných do provozu

Dlouhodobé cíle jsou uvedeny v následující tabulce ve struktuře navazující na **bod I.** v předcházejícím textu. Sloupec „atribut kvality“ specifikuje oblast, ke které cíl směřuje.

Oblast kvality	Kód cíle	Název cíle	Popis cíle	Atribut kvality
Kvalita zpracovávaných dat	CKN01	Zvýšení integrity dat	Používání robustních aplikací, integrovaných kontrolních mechanizmů do aplikací, kvalitní a aktuální provozní dokumentace, správné provedených migrací, kvalitní technické infrastruktury	Integrita dat
Kvalita zajišťovaných služeb	CKN02	Plnění funkčních požadavků	Průběžné sledování implementace, probíhajících testů a případně zkušebního provozu	Kvalita zajišťovaných služeb
	CKN03	Plnění provozních požadavků	Dodržení případně překročení provozních parametrů IS.	Kvalita zajišťovaných služeb
	CKN04	Uživatelská přívětivost IS	Maximální přizpůsobení požadavkům koncových uživatelů a pracovišť	Kvalita poskytovaných služeb
	CKN05	Uživatelské zvládnutí IS /aplikací/	Co nejlepší zvládnutí zaváděných programů koncovými uživateli.	Kvalita poskytovaných služeb
Kvalitní technická a programové infrastruktura	CKN06	Výběr a nasazení kvalitních technických a programových prostředků	Zajištění provedení kvalitního procesu pro výběr požadované kvality technických a programových komponent implementovaného informačního systému	Kvalita technických a programových prostředků

Tabulka 5-1 Dlouhodobé cíle kvality u zaváděných informačních systémů

5.1.2 Konkrétní cíle kvality u provozovaných IS

Dlouhodobé cíle jsou uvedeny v následující tabulce ve struktuře navazující na bod **II.** v předcházejícím textu. Sloupec „atribut kvality“ specifikuje oblast, ke které cíl směřuje.

Oblast kvality	Kód cíle	Název cíle	Popis cíle	Atribut kvality
Kvalita zpracovávaných dat	CKP01	Zvýšení integrity dat	Zajistit v IS kontrolní mechanizmy pro kontrolu zadávání údajů, provádět pravidelnou údržbu databází (kontrola konzistence dat), a kontrolovat a vyhodnocovat auditní logy	Integrita dat

	CKP10	Přesné údaje v evidencích a IS OVS	Při zadávání údajů do evidencí zadávat údaje s maximální přesností	Přesnost dat v ISVS
	CKP11	Údaje v evidencích a IS OVS jsou v souladu s obecně závaznými právními předpisy	Zajistit soulad s požadavky: Zák. č. 111/2009 Sb., o základních registrech, Zák. č.101/2000 Sb., o OOÚ; Zák. č. 106/1999 Sb., o svob. přístup k inf. a vyhl. č. 442/2006 Sb., struktura inf. zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup a vyhl. č. 64/2008 Sb., o přístupnosti	Soulad dat v ISVS s právními předpisy
	CKP12	Údaje jsou v ISVS OVS chráněné před zneužitím	Použití šifrovacích technologií	Utajitelnost dat
Kvalita zajišťovaných služeb	CKP02	Dostupnost napájení	Zajištění nepřerušitelného napájení elektrickou energií	Dostupnost zajišťovaných služeb
	CKP03	Efektivita systému	Zvýšení efektivity systému	Efektivnost služeb
	CKP04	Zlepšení systémové integrace	Zlepšení spolupráce informačních systémů / dílčích aplikací /	Interoperabilita služeb
	CKP05	Dostupnost služeb informačního systému	Zajištění vysoké dostupnosti služeb IS /odpovídající SLA a soubor technických a org. opatření/	Dostupnost služeb IS
	CKP06	HelpDesk	Zabezpečení kvalitního vyřizování hlášených problémů uživateli a jejich řešení	Dostupnost služeb IS
	CKP09	Web -Informační základna	Rozšíření informační základny poskytované prostřednictvím webového portálu, s cílem dále rozvíjet systém zveřejňování informací v rozsahu, který odpovídá vyhlášce č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup a v souladu se zájmy KK.	Rozšíření informační základny
Kvalita technických a programových prostředků	CKP07	Provozní stabilita a výkon	Zabezpečení provozní stálosti a výkonnosti systému.	Dostupnost služeb IS
	CKP08	Zjednodušení správy tech. a syst. infrastr.	Homogenizace operačních systémů a technické infrastruktury, konsolidace systémových a aplikačních logů	Efektivnost správy IS
	CKP13	Používání odpovídající síťové infrastruktury	Zajistit propojení všech lokálních počítačů vysoce propustnou sítí	Úroveň internetové konektivity

	CKP14	Software OVS je modifikovatelný a rozšiřitelný	Postupně vytvářet komplexní, modulární informační systém, vybavený flexibilním integračním rozhraním, s možností integrace dalších modulů, systémů, aplikací nebo webových služeb - podle aktuálních potřeb OVS.	Udržovatelnost a flexibilita ISVS
	CKP15	Software OVS je intuitivně komfortně ovladatelný	Zajistit soulad webového portálu / webových aplikací/ OVS s obecně očekávanými standardy ovládání aplikací	Použitelnost software ISVS

Tabulka 5-2 Dlouhodobé cíle kvality u provozovaných ISVS

5.2 Požadavky na kvalitu ISVS a PIS

Požadavky na kvalitu ISVS vznikly konkretizací výše stanovených cílů řízení kvality.

Souhrn požadavků na kvalitu informačních systémů typu ISVS a PIS, včetně vazeb na cíl, který naplňují, a vazeb na IS, pro které platí, je uveden v následující tabulce.

Cíl kvality	Označení požadavku na kvalitu	Popis požadavku	Platí pro
CKN01: zvýšení integrity dat	PK01	používání robustních aplikací, kvalitní a aktuální provozní dokumentace; správné provedených migrací, zajištění kvalitní technické infrastruktury	nově pořizované IS
CKN02: Plnění funkčních požadavků	PK02	Zajištění splnění požadavků na funkčnost IS / přehledný katalog uživatelských funkcí IS, testování klíčovými uživateli, proces akceptace apod./	nově pořizované IS
CKN03: Plnění provozních požadavků	PK03	Zajištění splnění požadavků na provoz implementovaných systémů /výkon, dostupnost, odezva, SLA- technická podpora, konzultační podpora atd./ - dodržení a případně překročení očekávaných provozních parametrů IS	nově pořizované IS
CKN04: Uživatelská přívětivost IS	PK04	Maximální přizpůsobení požadavkům koncových uživatelů a pracovišť	nově pořizované IS
CKN05: Uživatelské zvládnutí IS	PK05	Co nejlepší zvládnutí zaváděných programů koncovými uživateli /školení, trénink/	nově pořizované IS
CKN06: Výběr a nasazení kvalitních tech. a program. prostředků	PK06	Zajištění provedení kvalitního procesu pro výběr požadované kvality technických a programových komponent implementovaného informačního systému	nově pořizované IS
CKP01: zvýšení integrity dat	PK07	Homogenizace datové základny - využívání aplikací s co nejkompatibilnější datovou podporou, v rámci minimálního množství-pokud možno společných - podpůrných a databázových systémů	všechny IS v provozu
CKP02: dostupnost napájení	PK08	Zajištění náhradního systému pro dodávku el. energie v případě výpadku dodávky od standardního dodavatele (např. dieselagregát apod.)	všechny IS v provozu

Cíl kvality	Označení požadavku na kvalitu	Popis požadavku	Platí pro
CKP03: efektivita systému	PK09	Rozšíření možností vkládání datových vstupů, potřebných pro výkon administrativy státní a veřejné správy (podklady pro příslušná zpracování a úkony v informačních systémech) o možnosti zpracování dat přímo z aplikací s elektronickými formami kontaktu s veřejností (elektronické formuláře ve www aplikaci, přenosová rozhraní mezi www aplikacemi a informačními systémy jednotlivých organizačních útvarů, které příslušná data zpracovávají a na jejich základě vykonávají státní a veřejnou správu).	všechny IS v provozu
CKP04: zlepšení systémové integrace	PK10	Zlepšení kooperace dílčích informačních systémů /aplikací /	všechny IS v provozu
CKP05: Přístupová místa	PK11	Rozšíření počtu přístupových bodů pro zájemce, kteří nemají svůj vlastní přístup (informační kiosky, informační středisko s veřejným přístupem na internet případně s přístupem do informačního systému).	všechny IS v provozu
CKP06: Helpdesk	PK12	Zabezpečení kvalitního vyřizování hlášených problémů uživateli a jejich řešení	všechny IS v provozu
CKP07: provozní stabilita a výkon	PK13	Zabezpečení provozní stálosti a výkonnosti systému.	všechny IS v provozu
CKP08: zjednodušení správy tech.a syst.infrastr.	PK14	Homogenizace operačních systémů a technické infrastruktury, konsolidace systémových a aplikačních logů s cílem zjednodušení procesu správy systému.	všechny IS v provozu
CKP09: Web - informační základna	PK15	Rozšíření informační základny poskytované prostřednictvím webového portálu, s cílem dále rozvíjet systém zveřejňování informací v rozsahu, který odpovídá vyhlášce č. 442/2006 Sb., kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup a v souladu se zájmy KK	webový portál KK
CKP10: Přesné údaje v evidencích a IS orgánu veřejné správy	PK16	Při zadávání údajů do evidencí a informačních systémů zadávat data se zřetelem na maximální přesnost	všechny IS

Cíl kvality	Označení požadavku na kvalitu	Popis požadavku	Platí pro
CKP11: Údaje v evid. a IS OVS jsou v souladu s obecně platnými právními předpisy	PK17	Zjištění souladu s požadavky zák. č. 101/2000 Sb., o ochraně osobních údajů, zák. č. 106/1999 Sb. o poskytování veřejných informací, zák. č. 365/2000 Sb., o ISVS, ve znění pozdějších předpisů.	Všechny IS ISVS
CKP12: Údaje v IS jsou chráněny před zneužitím	PK18	Aplikace šifrovacích nástrojů a technologií.	IS určí OVS podle své potřeby - v souladu s §5b zák. o ISVS
CKP13: Používání odpovídající síťové infrastruktury	PK19	Zajištění propojení všech určených používaných počítačů vysoce propustnou sítí	Všechny IS
CKP14: Software OVS je modifikovatelný a rozšiřitelní	PK20	Rozvíjet stávající komplexní, modulární informační systém, vybavený flexibilním integračním rozhraním, s možností integrace dalších modulů, systémů, aplikací nebo webových služeb - podle aktuálních potřeb OVS.	Primárně pro nově pořizované IS
CKP15: Software OVS je intuitivně komfortně ovladatelný	PK21	Zajistit soulad webového portálu / webových aplikací/ OVS s obecně očekávanými standardy ovládání aplikací	Webové stránky

Tabulka 5-3 Souhrn požadavků na kvalitu ISVS a PIS

5.3 Plán řízení kvality ISVS a PIS

Činnosti v oblasti řízení kvality

V oblasti řízení kvality ISVS budou v rámci orgánu veřejné správy vykonávány činnosti, které jsou dále popsány v této části informační koncepce.

Stanovení cílů kvality:

- provádí zaměstnanec KK odpovědný za řízení kvality,
- zaměstnanec vymezí obecné cíle kvality, popíše je, přidělí jim příslušné atributy včetně požadovaného termínu naplnění a sestaví katalog cílů kvality,
- cíle kvality jsou součástí informační koncepce, tzn., mohou se měnit při změně verze IK.
-

Stanovení požadavků na kvalitu:

- zaměstnanec KK, odpovědný za řízení kvality, předá cíle kvality jednotlivým správcům IS,
- tito zaměstnanci pro každý cíl buď konstatují, že jejich IS již cíl splňuje, nebo sestaví požadavky, jejichž postupným splněním bude tento cíl naplněn,
- u požadavků si stanoví dílčí termíny takové, aby byl splněn termín požadovaného naplnění cíle,
- zaměstnanec, odpovědný za řízení kvality, požadavky sesbírá a vytvoří katalog požadavků na kvalitu, který se stává součástí informační koncepce.

Implementace požadavků na kvalitu:

- provádí dodavatel nebo vlastní zaměstnanec KK v závislosti na způsobu budování resp. údržby IS,
- zodpovídá na jedné straně zaměstnanec správce, na druhé straně vedoucí projektu,
- podklady čerpá z informační koncepce - platné verze,
- vychází z požadavků na kvalitu a časového harmonogramu jejich naplnění,
- dokončení implementace požadavku hlásí vedoucí projektu správce a ten dále informuje zaměstnance zodpovědného za naplňování IK.

Prověrka dodržování požadavků na kvalitu:

- provádí pověřený zaměstnanec KK,
- impuls dává zaměstnanec zodpovědný za naplňování IK,
- prověřuje se buď konkrétní implementace požadavku na konkrétním IS, nebo konkrétní požadavek na všech relevantních IS nebo všechny požadavky na vybraném IS apod.,
- z prověření se vytváří zápis, který obdrží zaměstnanec odpovědný za naplnění IK a zaměstnanec správce IS.

Vyhodnocení řízení kvality:

- provádí zaměstnanec odpovědný za naplnění IK, případně specialista na řízení kvality ISVS v organizaci,
- provádí se minimálně jednou za rok,
- součástí je vyhodnocení závěrů z provedených prověrek dodržování požadavků na kvalitu,
- provede se též revize dlouhodobých cílů kvality a jejich aktualizace,
- vyřadí se implementované a prověřené požadavky na kvalitu a vytvoří se nové,
- vyhodnocení může být podnětem k vydání nové verze IK.

Časový harmonogram řízení kvality

Časový plán procesu řízení kvality pro **nově pořizované a aktuálně zaváděné** informační systémy obou typů: ISVS i PIS, jsou součástí Plánů kvality standardní projektové dokumentace, která má respektovat rámcové obecné cíle kvality uvedené v aktuální verzi informační koncepce tohoto orgánu veřejné správy.

Podobně je tomu i u procesu řízení kvality dokumentu informační koncepce, kde namísto projektové dokumentace parametry kvality ověřuje pravidelnou periodickou kontrolou nařízenou ze zákona tento orgán veřejné správy. Detaily procesu přezkoumání plnění informační koncepce a její stále aktuálnosti pak specifikuje prováděcí vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy.

Cíl kvality	Obsah	Četnost
CKP01	Kontrola integrity (neporušenosti) a důvěrnosti dat	1xročně
CKN02	Prověrka plnění požadavků na funkčnost ISVS (a prověrka požadavků na změny)	1xročně
CKN02	Prověrka připomínek uživatelů a jejich zohlednění	1xročně
CKN03 CKP02	Prověrka spolehlivosti provozu systému (dostupnost zajišťovaných služeb, záznamy výpadků a odstávek).	4xročně
CKP03	Zvýšení efektivity provozu IS	1xročně
CKP04	Rozvoj systémové integrace	1x ročně
CKP05	Rozšíření počtu přístupových míst k IS	průběžně
CKP06	Kontrola účinnosti Helpdesku (řešení stížností a požadavků uživatelů)	1xročně
CKP07	Kontrola výkonnosti provozu IS (rychlost zpracování, odezvy systému, dodržování SLA)	1xročně
CKP08	Kontrola efektivnosti procesu správy systému	1xročně
CKP09	Web - informační základna	průběžně
CKP10	Přesné údaje v evidencích a IS orgánu veřejné správy	průběžně
CKP11	Údaje v evid. a IS OVS jsou v souladu s obecně platnými právními předpisy	řešeno následně s nabytím účinnosti
CKP12	Údaje v IS jsou chráněny před zneužitím	1xročně
CKP13	Používání odpovídající síťové infrastruktury	1xročně
CKP14	Software OVS je modifikovatelný a rozšiřitelní	1xročně
CKP15	Software OVS je intuitivně komfortně ovladatelný	1xročně

Tabulka 5-4 Časový harmonogram procesu řízení kvality informačních systémů

6 Řízení bezpečnosti ISVS

6.1 Výchozí stav informační bezpečnosti v rámci KK

6.1.1 Bezpečnostní dokumentace

Hlavním strategickým dokumentem v oblasti řízení bezpečnosti je Bezpečnostní politika informačního systému krajského úřadu Karlovarského kraje. V rámci BPIS KK je zpracována systémová bezpečnostní politika Karlovarského kraje. Svým určením a obsahem je SBPIS zaměřena na zajištění bezpečnosti odpovídající stanoveným požadavkům na zabezpečení provozovaného informačního systému, informací zpracovávaných v tomto IS, všech jeho jednotlivých komponent a oblastí, jež jsou dotčeny provozem informačního systému.

Bezpečnostní politika IS KK je součástí atestace dlouhodobého řízení dle zákona č. 365/2000 Sb., o ISVS (dle zákona o ISVS se jedná o bezpečnostní politiku ISVS)

Pomocí SBPIS KK 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.

6.1.2 Bezpečnost ISVS

Informační bezpečnost (bezpečnost IT/IS) lze obecně chápat jako zajištění:

- **důvěrnosti** (confidentiality) – vlastnost, že data nejsou dostupná nebo přístupná neautorizovaným osobám, entitám, nebo procesům,
- **integrity** (integrity) – vlastnost, že data jsou správná, tzn. například, že nebyla změněna nebo zničena neautorizovaným způsobem nebo vlastnost systému, že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautorizované manipulace se systémem,
- **dostupnosti** (availability) – vlastnost, že je něco na požádání přístupné a použitelné autorizovanou entitou.

Zajištění výše uvedených tři charakteristik bezpečnosti dat, spravovaných informačních systémů a služeb, které jsou jimi poskytovány, vyžaduje na OVS definice bezpečnosti podle § 5b zákona č. 365/2000 Sb., o ISVS, ve znění pozdějších předpisů.

Na řízení bezpečnosti IT/IS je třeba nahlížet jak na trvalý proces, používaný k dosažení a udržování příslušných úrovní výše zmíněných atributů bezpečnosti, tj. důvěrnosti, integrity, dostupnosti.

6.2 Dlouhodobé cíle v oblasti řízení bezpečnosti ISVS

Dlouhodobé cíle v oblasti řízení bezpečnosti informačních systémů veřejné správy byly KK stanoveny ve třech oblastech:

- **Zajištění bezpečnosti dat (informací)**, která jsou zpracovávána v rámci IS, u kterých je KK správcem dle zákona č. 365/2000 Sb., o ISVS.

- **Zajištění bezpečnosti služeb**, které jsou poskytovány IS, u kterých je KK správcem dle zákona č. 365/2000 Sb. o ISVS.
- **Zajištění bezpečnosti technických a programových prostředků**, které jsou použity v rámci ISVS, u kterých je KK správcem dle zákona č. 365/2000 Sb. o ISVS.

Konkrétní dlouhodobé cíle KK v oblasti řízení bezpečnosti ISVS jsou uvedeny v následující tabulce, a to v členění do tří výše uvedených oblastí. U každého cíle je dále uveden atribut bezpečnosti IS, ke kterému cíl směřuje.

Oblast řízení bezpečnosti ISVS	Označení cíle	Název cíle	Popis cíle
Bezpečnost dat, služeb, technických a programových prostředků	CB01	**Zajistit řízení bezpečnosti informací v souladu se standardy bezpečnosti**	Zajištění pravidelné aktualizace Příručky bezpečnosti KK s využitím nejnovějších bezpečnostních standardů, the best practicies a aktuálně platné legislativy.
	CB02	**Implementace opatření ke kontinuálnímu zlepšování bezpečnosti**	Postupná implementace navržených opatření ke zlepšování bezpečnosti
	CB03	**Audit ISMS**	Zajistit provedení auditu dle metodického pokynu

Tabulka 6-1 Dlouhodobé cíle v oblasti řízení bezpečnosti ISVS

6.3 Požadavky na bezpečnost ISVS

Požadavky na bezpečnost ISVS představují konkretizaci výše stanovených cílů řízení informační bezpečnosti, a to pro jednotlivé informační systémy KK, resp. záměry na vybudování nových IS, nebo jejich skupiny, případně pro všechny IS nebo záměry na jejich vybudování.

Souhrn požadavků včetně vazeb na cíle bezpečnosti, který naplňují, a vazeb na konkrétní IS KK, pro které platí, je uveden v následující tabulce.

Cíl bezpečnosti	Označení požadavku	Popis požadavku	Platnost pro ISVS/PIS
CB01	PB01	Provedení aktualizace **Příručky bezpečnosti informací** KK	Všechny ISVS a PIS KK
CB02 CB03	PB02	Aktualizace identifikace aktiv pro oblast řízení rizik a informační bezpečnosti KK, včetně technické infrastruktury, informačních aktiv ISVS a provozních IS (PIS). Zajistit pravidelnou aktualizaci analýzy rizik dle metodického pokynu k analýze rizik.	Všechny ISVS a PIS KK

Cíl bezpečnosti	Označení požadavku	Popis požadavku	Platnost pro ISVS/PIS
	PB03	Aktualizovat Registr informačních aktiv IS KK. Aktualizovat vlastníky aktiv včetně jejich povinností a odpovědností. Definovat a zavést do praxe pravidla pro přípustné použití informací a aktiv souvisejících s prostředky pro zpracování informací.	Všechny ISVS a PIS KK
	PB04	Aktualizovat klasifikační schéma informací IS KK. Aktualizovat pravidla pro označování a nakládání s informacemi.	Všechny ISVS a PIS KK
	PB05	Aktualizovat identifikaci rizik spojených s přístupem třetích stran (dodavatelů) a stanovit bezpečnostní požadavky, které musí být zohledněny ve všech současných i nových dohodách se třetími stranami.	Všechny ISVS a PIS KK
CB02	PB06	Udržovat průběžné povědomí uživatelů IS KK v oblasti bezpečnosti informací.	Všechny ISVS a PIS KK
	PB07	Provádět pravidelné prověřování obnovovacích postupů ze záložních médií a testování těchto médií.	Všechny ISVS a PIS KK
	PB08	Provádět pravidelné prověřování postupu pro správu vyměnitelných počítačových médií a jejich bezpečnou likvidaci.	Všechny ISVS a PIS KK
	PB09	Průběžné prověřování bezpečnostních pravidla a z nich plynoucí odpovědností pro uživatele IS KK a zajišťovat jejich dodržování.	Všechny ISVS a PIS KK
	PB10	Průběžné prověřování formálních pravidel na ochranu mobilní výpočetní techniky (zejména se jedná o používání prostředků pro šifrování informací) a vyhodnocovat jejich účinnost.	Všechny ISVS a PIS KK
	PB11	Průběžné prověřování pravidel pro práci na dálku (VPN) včetně požadavků nutných pro získávání tohoto druhu přístupu (závazek formou dodatku pracovní smlouvy).	Všechny ISVS a PIS KK
	PB12	Průběžné prověřování přístupových práv uživatelů IS KK.	Všechny ISVS a PIS KK
	PB13	Průběžné prověřování stávajících postupů pro hlášení a zvládání bezpečnostních událostí (incidentů, slabin apod.).	Všechny ISVS a PIS KK
CB02	PB14	Průběžné prověření kontinuity a havarijní plánování IS KK, včetně ověření funkcionality a účinnosti těchto plánů.	Všechny ISVS a PIS KK

Tabulka 6-2 Požadavky na bezpečnost ISVS

6.4 Plán řízení bezpečnosti ISVS

Plán řízení bezpečnosti ISVS obsahuje popis činností, které KK vykonává pro dosažení požadavků na bezpečnost ISVS, jejichž je správcem. Tento plán obsahuje i časový harmonogram plnění jednotlivých činností.

6.4.1 Činnosti v oblasti řízení bezpečnosti

V oblasti řízení bezpečnosti ISVS budou v rámci KK vykonávány činnosti, které jsou dále popsány v této kapitole.

Stanovení cílů bezpečnosti:

- provádí **zaměstnanec odpovědný za řízení bezpečnosti informací (dále jen bezpečnostní správce)**,
- tento zaměstnanec vymezí obecné cíle bezpečnosti, popíše je, přidělí jim příslušné atributy, včetně požadovaného termínu naplnění, a sestaví seznam cílů bezpečnosti,
- cíle bezpečnosti jsou součástí informační koncepce a mohou se měnit při změně verze informační koncepce v závislosti na aktuálních potřebách OVS.

Stanovení požadavků na bezpečnost:

- bezpečnostní správce předá cíle bezpečnosti správcům IS a/nebo projektovým manažerům odpovědným za rozvoj IS,
- tito zaměstnanci pro každý cíl buď konstatují, že daný IS již cíl splňuje, nebo sestaví požadavky, jejichž postupným splněním bude tento cíl naplněn,
- u požadavků si stanoví dílčí termíny takové, aby byl splněn termín požadovaného naplnění cíle,
- bezpečnostní správce tyto požadavky sesbírá a provede jejich posouzení s ohledem na celkovou bezpečnost IS KK, po jejich odsouhlasení následně vytvoří seznam požadavků na bezpečnost, který se stává součástí informační koncepce.

Implementace požadavků na bezpečnost:

- provádí dodavatel IS (v případě, že je IS poskytován jako služba) nebo vlastní zaměstnanec KK v závislosti na způsobu budování, resp. údržby IS,
- zodpovídá na jedné straně zaměstnanec správce IS (OVS), na druhé straně určený pracovník (např. vedoucí projektu) poskytovatele služeb,
- podklady jsou čerpány z platné verze informační koncepce,
- vychází se z požadavků na bezpečnost a časového harmonogramu jejich naplnění,
- dokončení implementace požadavku hlásí pověřený pracovník poskytovatele služeb (např. vedoucí projektu) zaměstnanci správce (KK), a ten dále informuje bezpečnostní správce a zaměstnance zodpovědného za naplňování informační koncepce.

Přezkoumání dodržování požadavků na bezpečnost:

- v pravidelných intervalech je prováděn interní audit ISMS schvalovaný vedoucím odboru projektového řízení a informatiky,

- prověřuje se buď konkrétní implementace požadavku na konkrétním IS, nebo konkrétní požadavek na všech relevantních IS nebo všechny požadavky na vybraném IS apod.,
- z provedeného interního auditu ISMS se vytváří zápis, který, obdrží bezpečnostní správce a představitel vedení KK.

Vyhodnocení řízení bezpečnosti:

- provádí bezpečnostní správce ve spolupráci bezpečnostním správcem a se zaměstnancem odpovědným za naplnění informační koncepce, případně jimi pověřený odborník na řízení ISMS,
- provádí se minimálně jednou za rok,
- součástí je vyhodnocení závěrů z provedených prověrek dodržování požadavků na bezpečnost,
- provede se též revize dlouhodobých cílů bezpečnosti a jejich aktualizace,
- vyřadí se implementovaná technická opatření na bezpečnost a navrhnou se nové,
- vyhodnocení může být podnětem k vydání nové verze informační koncepce.

6.4.2 Časové harmonogramy

Následující tabulka obsahuje časový harmonogram plnění dlouhodobých cílů v oblasti bezpečnosti ISVS.

Plánovaný termín dosažení cíle	Označení cíle	Název dlouhodobého cíle v bezpečnosti ISVS
1xza 4 roky	CB01	Aktualizace bezpečnostní politiky
kontinuálně	CB02	**Implementace opatření ke kontinuálnímu zlepšování bezpečnosti**
1xročně	CB03	Audit ISMS

Tabulka 6-3 Časový harmonogram plnění cílů v oblasti řízení bezpečnosti ISVS

Následující tabulka obsahuje časový harmonogram plnění požadavků na bezpečnost ISVS.

Plánovaný termín splnění požadavku	Označení požadavku	Popis požadavku na bezpečnost
1xročně	PB01	Provedení aktualizace **Příručky bezpečnosti informací** KK
1xročně	PB02	Aktualizace identifikace aktiv pro oblast řízení rizik a informační bezpečnosti KK, včetně technické infrastruktury, informačních aktiv ISVS a provozních IS (PIS). Zajistit pravidelnou aktualizaci analýzy rizik dle metodického pokynu Management rizik.
	PB03	Aktualizovat Registr aktiv IS KK. Aktualizovat vlastníky aktiv včetně jejich povinností a odpovědností.

Plánovaný termín splnění požadavku	Označení požadavku	Popis požadavku na bezpečnost
		Definovat a zavést do praxe pravidla pro přípustné použití informací a aktiv souvisejících s prostředky pro zpracování informací.
	PB04	Aktualizovat klasifikační schéma informací IS KK. Aktualizovat pravidla pro označování a nakládání s informacemi.
1xročně	PB05	Aktualizovat identifikaci rizik spojených s přístupem třetích stran (dodavatelů) a stanovit bezpečnostní požadavky, které musí být zohledněny ve všech současných i nových dohodách se třetími stranami.
1x za 3 roky nebo podle potřeby	PB06	Udržovat průběžné povědomí uživatelů IS KK v oblasti bezpečnosti informací.
Kontinuálně při provádění záloh	PB07	Provádět pravidelné prověřování obnovovacích postupů ze záložních médií a testování těchto médií.
1xročně	PB8	Provádět pravidelné prověřování postupu pro správu vyměnitelných počítačových médií a jejich bezpečnou likvidaci.
Průběžně, min 1xročně	PB9	Prověřování bezpečnostních pravidla a z nich plynoucí odpovědností pro uživatele IS KK a zajišťovat jejich dodržování.
1xročně	PB10	Prověřování formálních pravidel na ochranu mobilní výpočetní techniky (zejména se jedná o používání prostředků pro šifrování informací) a vyhodnocovat jejich účinnost.
1xročně nebo kontinuálně se změnami úvazků	PB11	Prověřování pravidel pro práci na dálku (VPN) včetně požadavků nutných pro získávání tohoto druhu přístupu (závazek formou dodatku pracovní smlouvy).
Průběžně, min 1xročně	PB12	Prověřování přístupových práv uživatelů IS KK.
1xročně	PB13	Prověřování stávajících postupů pro hlášení a zvládání bezpečnostních událostí (incidentů, slabin apod.).
1xročně	PB14	Prověření kontinuity a havarijní plánování IS KK, včetně ověření funkcionality a účinnosti těchto plánů.

Tabulka 6-4 Časový harmonogram plnění požadavků na bezpečnost

7 Zásady a postupy pro správu ISVS

7.1 Zásady a postupy pro pořizování a vytváření ISVS

KK (z kapacitních důvodů) pořizuje nový ISVS vždy dodávkou od externího dodavatele. Dodavatel zároveň zajišťuje systémovou integraci, komplexní testování a předání do provozu.

Pořizování ISVS je prováděno ve dvou rovinách:

a) **Vlastní záměr KK** – (vlastní iniciativa KK)
b) **Záměr jiného subjektu** – (např: MVČR)

Zásadními společnými hledisky pro implementaci IS bez ohledu na původ dodání jsou:

- Požadavky na úplnou a kvalitní dokumentaci IS
- Požadavky na kvalitní projektové řízení
- Podmínky akceptace
- Způsob servisu a provádění změn v systému

V případě dodávky ISVS od jiného subjektu, není KK schopno zcela zajistit dodržování podmínek stanovených v IK. Pořizování ISVS je v tomto případě prováděno dle požadavků daného subjektu.

Následující postup je využívám v případě, kdy se jedná o vlastní záměr KK pořízení ISVS.

7.1.1 Vypracování záměru nového ISVS

Zástupce KK vypracuje záměr dle postupu uvedeného v kap. 4. Následně postupuje dle metodiky nastavení řízení projektů.

7.1.2 Pořizování nového ISVS

V případě pořizování IS od dodavatele správce zajistí, aby součástí zadání bylo následující:

- požadavky na projektové řízení u dodavatele,
- požadavky na kvalitu a požadavky na bezpečnost, vyplývající z dlouhodobých cílů řízení kvality a dlouhodobých cílů řízení bezpečnosti,
- požadavky na testování,
- podmínky akceptace.
- požadavky na dokumentaci IS,
- nutná oprávnění pro provádění údržby a změn IS,

.

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

Zaměstnanec odpovědný za převzetí systému či jeho aktualizace, dohlédne na naplnění požadavku dodání provozní dokumentace v rámci dodávky IS. Uživatelé budou prokazatelně seznámeni se svými povinnostmi zakotvenými v provozní dokumentaci. Tato činnost bude opakována při každé změně provozní dokumentace. Povinnosti vyplývající z provozní dokumentace budou předmětem prověrek kvality.

7.2.1.2 Zásady a postupy vyhodnocování souladu provozování s požadavky vyhlášky

(Vyhodnocování souladu provozní dokumentace s §10 až §12 vyhlášky)

Součástí akceptace dodávky každé verze IS bude prověření obsahu provozní dokumentace na vyhláškou předepsané součásti. Vyhodnocování souladu provozování ISVS s IK a provozní dokumentací provádí 1x ročně prověrková komise v rámci pravidelných prověrek kvality.

7.2.1.3 Stanovení povinností osob v oblasti provozu a údržby

Zaměstnanci dodržují pravidla pro práci s ISVS. Při výskytu problému nahlásí danou událost prostřednictvím HelpDesku. Dodržují vyhlášené profylaktické kontroly a případné odstávky systému ohlášené správcem systému.

7.2.2 Řízení změn v ISVS

Řízení změn se vztahuje na případy, kdy je instalována nová verze IS se změněnými vlastnostmi nebo rozšířenou funkčností, nebo je při rutinní údržbě prováděn zásah, který nemá výsledný efekt na uživatelské vlastnosti.

Při implementaci verze je nezbytné zajistit:

- dokumentaci,
- proškolení všech dotčených skupin uživatelů
- zálohování a migraci dat,
- úplné testování, případně zkušební provoz (dle rozsahu),
- důslednou akceptaci.

Při realizaci změn v rámci údržby ISVS (např. zrychlení odezvy, update SW OS nebo DB) je nezbytné zajistit:

- seznámení správců se změnami ISVS
- bezpečnostní zálohování dat
- oznámení o případné odstávce systému a jeho opětovném spuštění
- důsledné testování

V případě zásadní změny je tato zpětně dokumentována do IK. Pro podrobné postupy při řízení změn se použijí odpovídající zásady uvedené v kapitole 7.1.

7.2.3 Ukončení činnosti ISVS

Ukončení činnosti ISVS je nutné plánovat v plánu rozvoje ISVS. V tomto plánu bude dokumentováno, jak bude činnost zajišťována ISVS dále prováděna, jakým systémem bude nahrazena, případně zda bude provedeno rušení bez náhrady a proč. Ukončení činnosti funkční ISVS je možné pouze dvěma způsoby:

1. Ukončení činnosti IS s náhradou jinou IS nebo upgrade stejné IS
2. Ukončení činnosti IS bez náhrady.

Oba případy mají jeden úkon společný. Je nezbytné zakonzervovat stav, ve kterém byla IS ukončena, zajistit bezpečné uložení programů a dat a následně včetně související dokumentace uložení do archivu. Případně se ukončení činnosti ISVS řídí dle licenčních podmínek konkrétního ISVS.

Dále je nutné oznámit ukončení činnosti této IS všem potenciálním uživatelům s tím, že se uvede náhrada stávající IS případně informační místo, které poskytne rady pro dosavadní uživatele (např. HelpDesk). Zajistí se stažení veškeré dokumentace a datových nosičů související s touto IS.

Pokud je činnost IS ukončena se současnou náhradou jinou IS nebo jejím upgrade, je o této situaci nutné uvědomit uživatele a zajistit náhrady programových médií a dokumentace (případně adekvátní formy při webovém provedení). Současně je nezbytné seznámit uživatele s případnou migrací dat a změnami v datových rozhraních.

Souhrnně je tedy nutné provést:

- seznámení potenciální skupin uživatelů (například veřejné oznámení na webu)
- zajištění bezpečné péče o data (převod, archivace, skartace, šifrování, anonymizace dat),
- jakým způsobem bude činnost ISVS fyzicky ukončena (např. likvidace záloh, médií, dokumentace, přístupů)
- vytvořit harmonogram ukončení
- zajistit kontinuitu služeb
- provést závěrečnou kontrolu a vytvořit protokol o ukončení činnosti ISVS.

7.3 Plánování rozvoje ISVS

Plánování rozvoje ISVS je realizováno v souladu se strategii KK nebo v případě zajištění okamžitých potřeb. (např.: v rámci nové legislativy)

Řízením rozvoje IS (včetně ISVS) je pověřen odbor OPI, který zajišťuje úkoly v rámci informatiky KK. OPI vytváří a průběžně udržuje **plán rozvoje ISVS**, který je upřesněním záměrů uvedených v IK.

Plán rozvoje ISVS obsahuje následující části:

- plán pořizování a vytváření nových ISVS,
- plán provozování a údržby provozovaných ISVS,

- plán provádění změn do stávajících ISVS,
- plán ukončení činnosti rušených ISVS.

Součástí plánu je přehled IS, které mají vzniknout, které mají být upraveny, které nahrazeny a které ukončeny bez náhrady. Dále bude v plánu uveden časový harmonogram provádění příslušných akcí v jednotlivých IS. Plán rozvoje ISVS je pravidelně aktualizován v souladu s dále uvedenými pravidly a na základě aktualizace požadavků v této oblasti.

Pravidla plánu rozvoje	
Za vytvoření plánu odpovídá	Vedoucí odboru projektového řízení a informatiky KK
Provádí plán a změny v něm	Tým pracovníků pověřený Vedoucím odboru projektového řízení a informatiky KK
Obsah navrhuje a dává podněty k provedení změn	Vedoucí odboru projektového řízení a informatiky KK
Schvaluje	Zastupitelstvo KK
Vyhodnocování plánu	1 x ročně

Tabulka 7-1 Pravidla pro vytváření plánu rozvoje ISVS

Prvotní plán rozvoje ISVS se vytváří na základě přípravy rozpočtu následujícího roku. Základem pro jeho naplnění jsou údaje uvedené v IK, především:

- informační systémy ve správě KK,
- záměry na pořízení nebo vytvoření nových ISVS,
- požadavky na kvalitu a časový harmonogram jejich naplnění,
- požadavky na bezpečnost a časový harmonogram jejich naplnění.

Plán rozvoje je dále doplněn informacemi získanými od vedoucích jednotlivých odborů KK, případně uživatelů jednotlivých IS. Dále probíhá pravidelná údržba plánu rozvoje prováděním následujících kroků:

- zjištění skutečného postupu prací v oblasti budování nových, změn a rušení stávajících ISVS,
- zjištění nových požadavků na nové ISVS, změny stávajících ISVS a ukončení činnosti provozovaných I ISVS,
- zjištění změn v parametrech plánu rozvoje ISVS (časové posuvy, změny priorit apod.),
- aktualizace obsahu plánu rozvoje ISVS,
- aktualizace harmonogramu rozvoje ISVS.

V případě zjištění závažných změn nebo požadavků na vytvoření nových významných ISVS může při aktualizaci plánu rozvoje ISVS vzniknout požadavek na vydání nové verze informační koncepce.

8 Způsob financování ISVS

Financování ICT (rozpočet ICT) v rámci KK je možné zajišťovat prostřednictvím tří základních zdrojů:

I. Finanční prostředky ze státního rozpočtu, které je možné dále členit na zdroje
   i. evidované prostřednictvím standardizovaného formuláře EDS/SMVS(dříve ISPROFIN[2]) /bez ohledu na to, zda se jedná o část investiční nebo provozní/ a to vždy tak, že ke každému projektu je vytvořen právě jeden záznam v EDS/SMVS; a/nebo
   ii. z přiznaného příspěvku příspěvkové organizace.

II. Vlastní zdroje (tzn. prostředky příspěvkových organizací mimo příspěvek na činnost a dotace z programového financování). Příkladem jsou prostředky získané vlastní činností (např. výzkumná, publikační činnost, aj. dle specifika a statutu organizace).

III. Jiné zdroje, což jsou prostředky jiné než předchozí dva. Příkladem jsou evropské (či jiné) finance u akcí a projektů řešených formou kofinancování[3], granty aj.

[3] Část celkové sumy ze státního rozpočtu (ISPROFIN) je zapisována v rámci finančních prostředků ze státního rozpočtu (viz zdroj I).

9 Naplňování Informační koncepce

9.1 Zásady

IK je dokument, který nastavuje cíle, metody a způsoby pro vytváření, řízení a provozování ISVS. Aby IK plnil funkci řídícího dokumentu je potřeba nakládat s ním takovým způsobem, aby se z něj nestal pouze formální dokument, což představuje provádění následujících akcí:

- Realizace - Praktické naplnění postupů a zásad uvedených v IK
- Aktualizace - Udržování IK v aktuálním stavu
- Vyhodnocení - Pravidelné vyhodnocování dodržování informační koncepce a realizaci opatření pro odstranění zjištěných nedostatků

Pro zajištění praktického naplnění postupů a zásad uvedených v IK je třeba stanovit osobní odpovědnosti za jednotlivé oblasti, které IK řeší. Odpovědnost je dána maticí odpovědnosti uvedené v kapitole 10.

9.2 Praktické naplnění postupů a zásad uvedených v IK

Proto, aby byla IK využita ke svému účelu a „vstřebána“ do operativního řízení KK a stala se součástí pravidelných činností. Jsou součástí realizace IK následující postupy:

- Zavedení
- Vyhlášení

9.2.1 Zavedení

Kromě zaměstnanců, kteří stojí u zrodu IK a jejího projednávání se realizace účastní další zaměstnanci, kteří budou garantovat to, že IK bude přijata jako interní směrnice a prováděny správcovské úkony, které jsou dále popsány v této kapitole. Tito zaměstnanci jsou uvedeni v kapitole 10 a **odpovídají za provádění předepsaných úkolů** bez ohledu na to, zda budou prováděny nahodile, nebo v předepsané frekvenci. Jejich vedoucí pak budou odpovídat za to, že to skutečně provádí.

9.2.2 Vyhlášení

Zaměstnanci KK, kterých se IK dotýká, musí být informování o tom, že se tato směrnice začala používat, a že tak bude nadále, pokud nebude dalším výrokem zrušena. Musí být seznámeni se způsobem označování IK (verze) a aktualizací i tím, že další ohlašování se již týká oblasti aktualizace IK.

Součástí informací musí být oznámení o místě uložení a její fyzické dostupnosti. S dokumentem se zachází stejně, jako s dokumenty kvality, tzn., doporučuje se, aby neřízené kopie dokumentu nebyly vytvářeny, nebo pouze v odůvodněných případech. Tak se předejde nebezpečí, že mezi uživateli se budou pohybovat již neplatné, nebo zastaralé verze. Ideální stav je omezení přístupu pouze prostřednictvím sdíleného přístupu k centrálně uloženému dokumentu.

9.3 Udržování IK v aktuálním stavu

Standardním postupem aktualizace jsou následující kroky:

- Zjištění změn
- Včasná reakce na změny
- Změna IK
- Vytvoření nové IK

9.3.1 Zjištění změn s dopadem na IK

Pro zjištění změn v oblastech, které se dotýkají IK, se použijí následující postupy, které je nutné zavést do operativní činnosti:

- Upozornění na potřebu změn od vedoucích odborů používajících sledované ISVS
- Upozornění na potřebu změn od správců sledovaných ISVS
- Sběr podnětů a reklamací uživatelů shromažďovaných na výše uvedených místech (HelpDesk).
- Výsledky kontrolních akcí prováděných auditorským týmem
- Podněty příslušných zaměstnanců KK
- Vnější podněty

Postupy budou prováděny v rámci

- periodických kontrol IK
- mimo termín v případě naléhavé nutnosti
- v případě fatálních selhání systému neprodleně

Přednostně se provádějí pravidelné kontroly v intervalech 12 měsíců, při kterých se zaregistrují všechny požadavky na aktualizaci shromážděné v průběhu období.

Změny se pak promítají do IK podle důležitosti těmito způsoby:

- provedením změny v IK resp. vydání její nové verze,
- schválením změny IK resp. její nové verze,
- přípravou nové informační koncepce v předstihu před ukončením platnosti té stávající.

9.3.2 Postup pro zajištění včasné změny IK

Pro zajištění včasné aktualizace IK bude prováděna její revize s periodou 1 x ročně. Tato perioda bude časově sladěna s periodou vyhodnocování IK s hlediska dodržování tak, aby mohla být do nové verze IK zároveň zahrnuta schválená opatření. Mimo tuto pravidelnou revizi bude IK změněna též v případě:

- vzniku nového záměru na pořízení nebo vytvoření ISVS,
- uvedení nového ISVS do rutinního provozu,

- uvedení nové verze ISVS, která významným způsobem změní obsažená data anebo zajišťované služby, do provozu
- ukončení činnosti ISVS,
- zásadní změny právních předpisů v oblasti dlouhodobého řízení ISVS,
- zásadní změně organizační struktury KK s přímým vlivem na odpovědnosti v oblasti dlouhodobého řízení ISVS.

V této souvislosti musí řídící zaměstnanci všech útvarů, které spravují některý ISVS, hlásit výše uvedené změny související s jimi spravovaným ISVS zaměstnanci odpovědnému za přípravu změn a tvorbu nových verzí IK. Tento zaměstnanec je též povinen sledovat další výše uvedené změny a jejich dopad na informační koncepci.

9.3.3 Záznam změny v dokumentu IK

Změny IK je přípustné provádět výlučně vydáním její nové verze, každá verze IK je průkazně označena (číslována).

Formát čísla verze je VXX.YY, kde

XX je číslo verze

YY je číslo dílčí verze v rámci verze

Členění na dílčí verze se použije v případě, kdy hlavní verze bude aktualizována drobnějšími změnami (např. změny v personální oblasti, drobná změna v postupech apod.).

V identifikační části IK se vloží nová tabulka s identifikačními údaji, která obsahuje:

- číselné označení verze viz výše,
- datum vzniku verze,
- datum schválení verze,
- datum počátku platnosti verze,
- autor verze IK, který provedl schválené změny
- osobu, útvar, který schválila verzi IK,
- podpis zástupce KK,
- název souboru, umístění souboru (na intranetu, sdíleném disku apod.),
- počet stran a počet případných příloh.

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

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

9.3.4 Postup schvalování změny IK

Novou verzi IK schvaluje osoba stanovená v kapitole 10. Verzi je třeba předložit ke schválení s předstihem před požadovaným vstupem v platnost, doporučeno je ***10 dní.***

Vyhlášení nové verze se provede způsobem, běžným u systémů jakosti, tzn.:

- s novou verzí budou prokazatelně seznámeni všichni zaměstnanci, jichž se nějak dotýká,
- zaváží se starou verzi nadále nepoužívat.

Prokazatelné seznámení zaměstnanců KK se provede dle obvyklého procesu seznamování s interními předpisy na KK. Např. podpisová listina, závazné interní sdělení atd.

9.3.5 Postup přípravy nové IK

Zaměstnanec odpovědný za naplnění IK připraví ***6 měsíců*** před ukončením její platnosti podklady pro strategické rozhodnutí **vedoucího odboru projektového řízení a informatiky KK** ohledně přípravy nové informační koncepce. Tyto podklady budou obsahovat:

- vyhodnocení stávající informační koncepce a její účinnosti za dobu od jejího vzniku,
- vyhodnocení způsobu vzniku a údržby stávající IK a doporučení pro postup tvorby nové (vlastními silami nebo s využitím externího dodavatele apod.),
- další relevantní podklady dle uvážení zaměstnanců.

Vedoucí OPI rozhodne o dalším postupu.

9.4 Vyhodnocení IK

9.4.1 Hodnotitel

Pracoviště, které má na starosti kontrolu závazků vyplývajících z informační koncepce, podává zprávu o kontrole stavu jako součást hlášení o stavu ICT.

Vyhodnocování dodržování informační koncepce je základním kontrolním mechanizmem zajišťujícím zpětnou vazbu. Základní pravidlo platné pro oblast vyhodnocování je takové, že vyhodnocování musí provádět jiný zaměstnanec než ten, který je zodpovědný za naplňování informační koncepce.

9.4.2 Mimořádné vyhodnocení IK

Mimořádné hodnocení je realizováno v případě potřeby zjištění daného stavu naplňování IK. Mimořádné může být iniciováno vedoucím OPI, nebo interním auditorem KK v rámci hodnocení stavu informačních systémů.

Postup mimořádného hodnocení je popsán v kapitole 9.4.4

9.4.3 Pravidelné vyhodnocení IK

Pravidelné vyhodnocení IK zajišťuje jednak dodržování požadavků kvality a současně zpětnou vazbu pro vedení instituce. Na základě tohoto vyhodnocení se následně provádějí případné změny a aktualizace, jak je popsáno v kapitole 9.3. Termín pro provádění

vyhodnocení je ***1x za rok***. Konání vyhodnocení by mělo být sladěno s periodou aktualizací IK tak, aby se opatření přijatá na základě vyhodnocení stala předmětem pravidelné aktualizace IK.

Všechny činnosti, jejichž provádění je posuzováno, jsou porovnávány s IK platnou v době, kdy byla daná činnost prováděna – na to je nutné dbát v případě, že došlo za uplynulých 12 měsíců ke změně IK. Vyhodnocení se provádí v jednotlivých částech IK (viz. kapitola 9.4.5).

9.4.4 Postup vyhodnocení IK

Zaměstnanec, případně externí subjekt, který provádí vyhodnocování IK, vytvoří záznam o průběhu vyhodnocování. Záznam bude obsahovat položky:

- oblasti hodnocení
- splnění požadavku,
- dopad na přípravu, řízení a provoz ISVS,
- odpovědnost za vzniklý stav,
- doporučení pro řešení (způsob, rozsah, nástroje),
- doporučení maximálního termínu k vyřešení,
- doporučení na kontrolu realizace opatření,
- komentář k hodnocení.

9.4.5 Oblasti hodnocení IK

Přednostně se v IK hodnotí obsahová shoda s požadavky zákona, tzn. zda IK obsahuje následující podstatné části a jejich obsah je aktuální:

9.4.5.1 Identifikace ISVS

Zjišťuje se a hodnotí, zda:

- jsou charakteristiky všech ISVS úplné,
- je seznam provozních IS s vazbami na ISVS úplný,
- je prováděna včasná aktualizace charakteristiky současného stavu,
- je prováděna včasná aktualizace předpokládaných změn IS.

9.4.5.2 Záměry na pořízení nebo vytvoření nových ISVS

Zjišťuje se a hodnotí, zda:

- IK 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.

9.4.5.3 Řízení kvality

Zjišťuje se a hodnotí, zda:

- požadavky na kvalitu směřují k naplnění cílů kvality,
- požadavky na kvalitu jsou jednotlivými IS dodržovány a vyhodnocovány,
- probíhá prověrka požadavků na kvalitu a vyhodnocení řízení kvality v souladu s plánem řízení kvality.

9.4.5.4 Řízení bezpečnosti

Zjišťuje se a hodnotí, zda:

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

9.4.5.5 Správa a provoz ISVS

Zjišťuje se a hodnotí, zda:

- jsou uplatňovány zásady a postupy pro plánování rozvoje ISVS.
- je výběr formy budování nového ISVS 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 IK 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 řízeni jsou uplatňovány přijaté zásady v této oblasti.
- 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.

9.4.5.6 Financování ISVS

Zjišťuje se a hodnotí zda::

- 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.

9.4.5.7 Aktualizace a změny IK

Zjišťuje se a hodnotí, zda:

- jsou dodržovány termíny periodické aktualizace,
- jsou do IK promítány i zásadní změny jsou promítány mimo pravidelné aktualizace,
- vydávání nových verzí IK probíhá v souladu s danými postupy,
- jsou verze a v nich zahrnuté změny jsou náležitě dokumentovány, schvalovány a vyhlášen,
- všichni dotčení zaměstnanci mají k dispozici aktuální platnou verzi IK,
- nejsou používány neplatné verze IK.

9.4.5.8 Vyhodnocení IK

Zjišťuje se a hodnotí, zda:

- vyhodnocení od posledního vyhodnocení neuběhlo více než je předepsaná doba
- záznamy z minulých vyhodnocení jsou dostupné obdobně, jako aktuální verze IK,
- byly do aktuální verze IK promítnuty opatření přijatá při minulém vyhodnocení IK,
- jsou přijatá opatření uplatňována v praxi,
- přijatá opatření přinesla předpokládaný účinek (nedostatky byly odstraněny nebo jsou odstraňovány).

9.4.5.9 Matice odpovědnosti

Zjišťuje se a hodnotí, zda:

- odpovídá matice odpovědnosti skutečnému stavu
- jsou stanoveny funkce odpovědnosti dle IK
- proběhlo prokazatelné seznámení osob uvedených v matici odpovědnosti s IK

9.4.5.10 Prověrka připomínek uživatelů

Zjišťuje se a hodnotí, zda:

- jsou řešeny připomínky uživatelů IK

9.4.6 Záznam o vyhodnocení IK

Záznam o vyhodnocení IK je záznamem sledování kvality systému. Jedná se o řízený dokument, jehož vydání je sledováno a je spolu s ostatními dokumenty kvality archivován.

Odpovědnost za vytvoření záznamu má zaměstnanec odpovědný za provádění kontrol IK určený v kapitole 10.

Do záznamu se zaznamená:

- identifikace hodnocené IK
    - název instituce,

- datum počátku platnosti hodnocené IK,
- verze IK,
- pořadové číslo zápisu,
- Hodnotitel (identifikace zaměstnanců, kteří hodnotili jejich role, jména, útvar nebo externí organizace),
- datum záznamu,
- datum schválení,
- Schvalovatel záznamu.

- záznam o průběhu vyhodnocení (dle jednotlivých oblastí)
- výsledky z vyhodnocení (soupis zjištěných nedostatků)
- návrh opatření (soupis navržených opatření, termíny realizace, termíny kontroly)
- závěry z hodnocení

9.4.7 Nápravná opatření

9.4.7.1 Opatření k nápravě

Opatření k nápravě se týká odhalených vad, nedodělků a neshod v průběhu naplňování IK. Pokud je při vyhodnocování IK zjištěna situace, která vyžaduje přijetí nápravného opatření, provede se zápis do záznamu o průběhu vyhodnocení, kde se uvede popis neshody dle předepsaných položek - viz kap.: 9.4.5.

9.4.8 Schválení hodnocení

Závěry hodnocení a návrhy opatření jsou vloženy do záznamu a ten je předložen vedoucím kontrolního týmu odpovědnému zaměstnanci.

Schválený záznam se zpřístupní a všichni dotčení zaměstnanci se s ním seznámí prokazatelným způsobem, jako u nové verze IK.

Opatření s vlivem na obsah IK se promítnou v nejbližší řádné aktualizaci.

10 Matice zodpovědnosti a plnění zákonných povinností

Informační koncepce je řídící dokument, který je účinný pouze tehdy, je-li provozován za neustálého dohledu. K tomu, aby plnila svoji funkce v systému řízení ISVS KK, jsou určeni zaměstnanci KK, kteří odpovídají za provádění a kontrolní činnosti IK.

Ty lze rozčlenit do dvou skupin:

1. Odpovědnosti za realizaci vlastní informační koncepce KK,
2. Odpovědnosti za plnění zákonných povinností vyplývajících ze zákona č. 365/2000Sb., o ISVS

Rámcově platí tato odpovědnost

- Zaměstnanec určený pro konkrétní funkci (doporučuje)
- Vedoucí odboru projektového řízení a informatiky KK (schvaluje)

10.1 Odpovědnosti za realizaci informační koncepce (matice odpovědnosti)

Za realizaci IK jako celku odpovídá **odbor projektového řízení a informatiky KK.** V rámci práce s informačními systémy jsou na OPI stanoveny následující funkce:

- Správce IK
- Správce konkrétního informačních systémů – Správce IS
- Bezpečnostní správce systému
- Projektový manažer

Tyto funkce se nemusí krýt s pozicemi organizačního řádu KK a mohou být sloučeny s výkonem jiných činností v rámci organizace. Přidělení daných funkcí v rámci činností plynoucí z IK je v pravomoci vedoucího odboru informatiky dané organizace.

Souhrn činností popsaných v IK je uveden v následující tabulce:

ID	ČINNOSTI	REALIZUJE
1	Vytváření záměrů na nové IS	Vedoucí OPI.
2	Schvalování záměrů	Zastupitelstvo KK
3	Řízení kvality ISVS	Projektový manažer
4	Řízení bezpečnosti ISVS	Bezpečnostní správce
5	Řízení postupů pro pořizování a vytváření ISVS (včetně zajištění veřejných soutěží apod.)	Projektový manažer
6	Koordinace činností v oblasti rozvoje ISVS.	Projektový manažer
7	Příprava plánu rozvoje ISVS.	Vedoucí OPI.
8	Schvalování plánu rozvoje ISVS.	Zastupitelstvo KK
9	Zajištění provozu a údržby ISVS.	Správci IS
10	Vyhodnocování souladu provozování ISVS s IK.	Nezávislý subjekt
11	Koordinace a vyhodnocování řízení změn.	Vedoucí OPI
12	Řízení ukončování provozu IS.	Projektový manažer
13	Vytváření a údržba plánu financování ISVS.	Vedoucí OPI
14	Schvalování plánu financování ISVS.	Rada KK
15	Příprava změn a tvorba nových verzí IK.	Správce IK
16	Schvalování změn IK a jejích nových verzí.	Vedoucí OPI
17	Příprava nové IK před ukončením platnosti stávající.	Správce IK
18	Prověrky dodržování IK a návrh opatření na základě zjištění prověrek.	Nezávislý subjekt
19	Schvalování záznamů z prověrek.	Vedoucí OPI
20	Schvalování nápravných a preventivních opatření.	Vedoucí OPI

Tabulka 10-1 Souhrn činností

10.2 Plnění zákonných povinností

Zastřešující vrcholovou odpovědnost za plnění zákonných povinností vyplývajících ze zákona č.365/2000 Sb., o ISVS má **vedoucí odboru projektového řízení a informatiky KK.** Realizaci konkrétních činností dané zákonem č.365/2000 Sb., o ISVS pověřuje zaměstnance OPI.

Povinnosti OVS dané zákonem č.365/2000 Sb., o ISVS jsou uvedeny v následující tabulce.

Povinnost dle zákona	Úkol
Zák. č. 365/2000 Sb. §5 odst. 2 písm. a.	Spolupracovat s Ministerstvem vnitra při plnění jeho úkolů podle § 4 odst. 1.
Zák. č. 365/2000 Sb. §5 odst. 2 písm. a.	Spolupracovat s Ministerstvem vnitra při provádění kontroly na místě dle zákona o státní kontrole.
Zák. č. 365/2000 Sb. §5 odst. 2 písm. b.	Předložit Ministerstvu vnitra k vyjádření návrhy dokumentací programů obsahující pořízení, obnovu a provozování informačních a komunikačních technologií.
Zák. č. 365/2000 Sb. §5 odst. 2 písm. b.	Předložit Ministerstvu vnitra k vyjádření investiční záměry akcí pořízení, obnovy a provozování informačních a komunikačních technologií - přesné podmínky viz zákon.
Zák. č. 365/2000 Sb. §5 odst. 2 písm. c.	Uveřejňovat číselníky, pokud jsou jejich správci a není zákonem stanoveno jinak, a to i způsobem umožňujícím dálkový přístup.
Zák. č. 365/2000 Sb. §5 odst. 2 písm. c.	Předávat Ministerstvu vnitra údaje do informačního systému o datových prvcích v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem.
Zák. č. 365/2000 Sb. §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.
Zák. č. 365/2000 Sb. §5 odst. 2 písm. d.	Prokázat atestem způsobilost informačního systému k realizaci výše uvedených vazeb.(upřesňuje vyhláška č. 53/2007 Sb.)
Zák. č. 365/2000 Sb. §5 odst. 2 písm. e.	Zpřístupňovat ministerstvu v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem, bez zbytečného odkladu informace o jimi provozovaném informačním systému a jím poskytovaných službách a používaných datových prvcích, a to za účelem uveřejnění v IS o ISVS a IS o DP. Web adresa portálu: http://www.sluzby-isvs.cz (upřesňuje vyhláška č. 528/2006 Sb. a upřesňuje vyhláška č. 469/2006 Sb.).
Zák. č. 365/2000 Sb. §5 odst. 2 písm. f.	Postupovat při uveřejňování informací způsobem umožňujícím dálkový přístup tak, aby byly informace související s výkonem veřejné správy uveřejňovány ve formě, která umožňuje, aby se s těmito informacemi v nezbytném rozsahu mohly seznámit i osoby se zdravotním postižením. (upřesňuje vyhláška č.64/2008)
Zák. č. 365/2000 Sb. §5 odst. 2 písm. g.	Odstranit zjištěné nedostatky ve lhůtě stanovené Ministerstvem vnitra.
Zák. č. 365/2000 Sb. §5a odst. 1.	Vytvářet a vydávat informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování.
Zák. č. 365/2000 Sb. §5a odst. 2.	Vytvářet a vydávat provozní dokumentaci k jednotlivým ISVS, uplatňovat ji v praxi a vyhodnocovat její dodržování.
Zák. č. 365/2000 Sb. §5a odst. 3.	Zajistit atest dlouhodobého řízení ISVS.

Tabulka 10-2 Přehled plnění zákonných povinností

11 Závěrečné shrnutí

Informační koncepce představuje řídící dokument na KK řízení pro oblasti ISVS. Po schválení dokumentu odpovědným útvarem KK je nutné zahájit atestační řízení u pověřeného atestačního střediska pro oblast atestací ISVS. Výsledkem atestačního řízení je získání atestu Dlouhodobého řízení ISVS.

Prvním krokem pro úspěšné řízení ISVS je seznámení zaměstnanců s IK a její zavedení do praxe. Pro odstranění prvotních nedostatků zjištěných při použití IK, je doporučeno provést mimořádné hodnocení. Výsledkem bude aktualizace dokumentu vytvořením nové verze IK, kde budou odstraněny zjištěné nedostatky. Dále je již možno provádět pravidelné vyhodnocení dle postupu uvedeném v IK.

Důležitým krokem je neustálé provádění kontrol dle IK a udržování IK v aktuálním stavu.