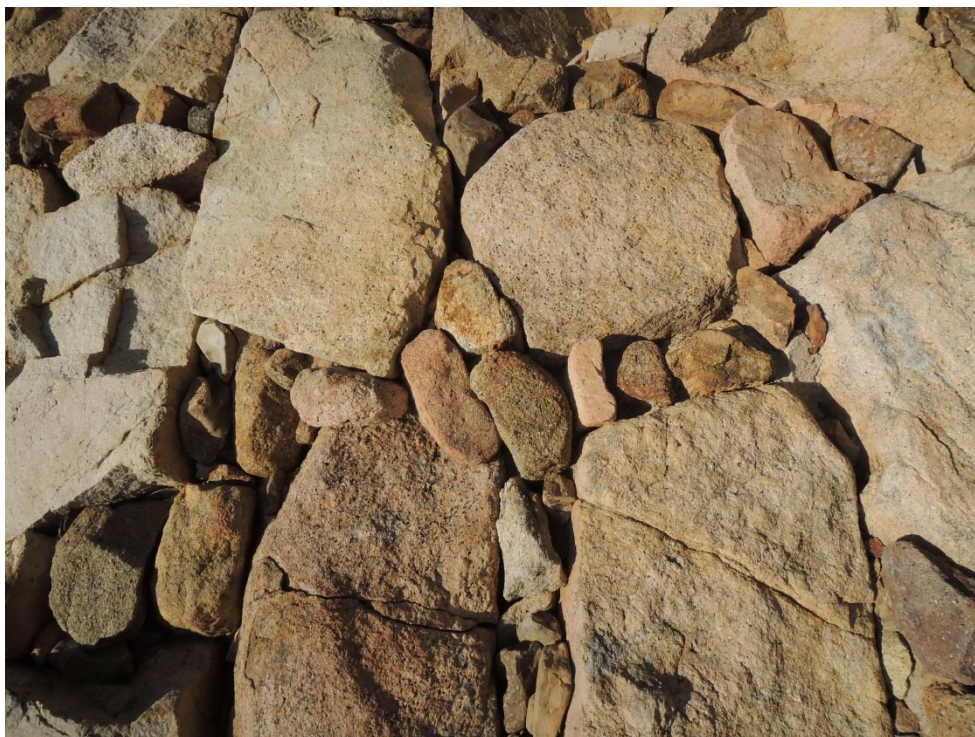


# Olomoucký kraj



## Informační koncepce

<b>Popis:</b>	Informační koncepce
<b>Zpracovali:</b>	viz strana číslo 6
<b>Verze:</b>	2.0
<b>Status:</b>	Schváleno
<b>Počet stran:</b>	41
<b>Dne:</b>	15. 1. 2016
<b>Platnost od:</b>	1. 12. 2014
<b>Schválil:</b>	Mgr. Lucie Štěpánková
<b>Klasifikace:</b>	Interní informace
<b>Umístění:</b>	Intranet – soubor: informační koncepce 2.0

## Obsah

<b>1</b>	<b>ÚVOD</b>	<b>4</b>
1.1	PŘEDMĚT, ÚČEL A CÍL INFORMAČNÍ KONCEPCE	4
1.1.1	<i>Předmět informační koncepce</i>	4
1.1.2	<i>Účel informační koncepce</i>	4
1.1.3	<i>Cíl informační koncepce</i>	4
1.2	ROZSAH A PLATNOST INFORMAČNÍ KONCEPCE	4
1.2.1	<i>Určení hranic informačního systému</i>	4
1.2.2	<i>Závaznost informační koncepce</i>	4
1.2.3	<i>Vazby informační koncepce</i>	5
1.2.4	<i>Legislativní rámec informační koncepce</i>	5
1.3	ORGANIZACE DOKUMENTU	6
1.3.1	<i>Základní údaje</i>	6
1.3.2	<i>Verze 2.0 - aktuální verze informační koncepce</i>	6
1.3.3	<i>Verze 1.2</i>	7
1.3.4	<i>Verze 1.1</i>	8
1.3.5	<i>Verze 1.0 - výchozí verze informační koncepce</i>	8
1.3.6	<i>Struktura dokumentu</i>	9
1.4	PŘEHLED ZKRATEK	9
<b>2</b>	<b>POPIS ISVS</b>	<b>11</b>
<b>3</b>	<b>ZÁMĚRY NA POŘÍZENÍ NEBO VYTVOŘENÍ NOVÝCH IS</b>	<b>13</b>
3.1	PLÁN ROZVOJE IS	13
<b>4</b>	<b>ŘÍZENÍ KVALITY IS</b>	<b>14</b>
4.1	ÚČEL IS	14
4.1.1	<i>Základní principy</i>	14
4.1.2	<i>IS jako nástroj</i>	14
4.1.3	<i>IS jako služba</i>	15
4.2	DLOUHODOBÉ CÍLE V OBLASTI ŘÍZENÍ KVALITY IS	15
4.3	POŽADAVKY NA KVALITU IS	17
4.4	PLÁN ŘÍZENÍ KVALITY IS	19
<b>5</b>	<b>ŘÍZENÍ BEZPEČNOSTI IS</b>	<b>23</b>
5.1	ZÁKLADNÍ PRINCIPY	23
5.2	DLOUHODOBÉ CÍLE V OBLASTI ŘÍZENÍ BEZPEČNOSTI IS	24
5.3	POŽADAVKY NA BEZPEČNOST IS	24
5.4	PLÁN ŘÍZENÍ BEZPEČNOSTI IS	25
<b>6</b>	<b>ZÁSADY A POSTUPY PRO SPRÁVU IS</b>	<b>29</b>
6.1	ZÁSADY A POSTUPY PRO POŘIZOVÁNÍ A VYTVÁŘENÍ IS	29
6.1.1	<i>Vytváření IS</i>	29
6.1.2	<i>Pořizování IS</i>	29
6.2	ZÁSADY A POSTUPY PRO PROVOZOVÁNÍ IS	30
6.3	ŘÍZENÍ ZMĚN V IS	31
6.4	UKONČENÍ ČINNOSTI IS	32
<b>7</b>	<b>FINANCOVÁNÍ IS</b>	<b>33</b>
<b>8</b>	<b>NAPLŇOVÁNÍ INFORMAČNÍ KONCEPCE A ŘÍZENÍ ZMĚN</b>	<b>34</b>
8.1	DODRŽOVÁNÍ INFORMAČNÍ KONCEPCE	34
8.2	KONTROLA DODRŽOVÁNÍ INFORMAČNÍ KONCEPCE	34
8.2.1	<i>Oblasti pro kontrolu dodržování informační koncepce</i>	34

8.2.2	<i>Zápis z kontroly dodržování informační koncepce.....</i>	35
8.3	ŘÍZENÍ ZMĚN INFORMAČNÍ KONCEPCE.....	36
<b>9</b>	<b>ORGANIZACE ŘÍZENÍ A ODPOVĚDNOSTI .....</b>	<b>37</b>
9.1	ZÁKLADNÍ PRINCIPY ŘÍZENÍ KVALITY A BEZPEČNOSTI IS .....	37
9.2	VÝKON ŘÍZENÍ KVALITY A BEZPEČNOSTI IS .....	37
9.2.1	<i>Řízení realizace informační koncepce.....</i>	37
9.2.2	<i>Řízení činností ke splnění zákonných povinností .....</i>	38
<b>10</b>	<b>SEZNAM PŘÍLOH .....</b>	<b>41</b>

# 1 Úvod

## 1.1 Předmět, účel a cíl informační koncepce

### 1.1.1 Předmět informační koncepce

Tato informační koncepce byla vypracována zejména na základě zákona č. 365/2000 Sb. a vyhlášky č. 529/2006 Sb. Předmětem tohoto dokumentu je implementace požadavků na řízení a kontrolu všech činností souvisejících s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy.

### 1.1.2 Účel informační koncepce

Účelem je zavedení **systematického přístupu** k budování a provozování informačního systému veřejné správy jako základního podpůrného prostředku pro plnění hlavních cílů krajského úřadu v oblasti jeho působnosti – tj. především pro zajištění **vysoké kvality výkonu samosprávy a státní správy a služeb** občanům Olomouckého kraje.

### 1.1.3 Cíl informační koncepce

Cílem je **definování hlavních principů a nastavení a zavedení procesů**, které budou ošetřovat řízení kvality a bezpečnosti informačního systému veřejné správy, tj. principů a procesů pro dosažení **vysoké kvality a bezpečnosti dat** zpracovávaných v informačním systému a **vysoké kvality a bezpečnosti služeb** tímto systémem poskytovaných.

Podrobněji jsou cíle, požadavky a jednotlivé činnosti popsány dále zejména v kapitolách 4 - Řízení kvality IS a 5 - Řízení bezpečnosti IS.

## 1.2 Rozsah a platnost informační koncepce

### 1.2.1 Určení hranic informačního systému

Informační koncepce se vztahuje na všechny informační systémy, které tvoří informační systém veřejné správy (ISVS) krajského úřadu tak, jak je dále popsán v následujících kapitolách – zvláště viz kapitola 2 - Popis ISVS a Příloha č. 1. Na ostatní (tzv. provozní) informační systémy spravované krajským úřadem se tato informační koncepce vztahuje z hlediska vazeb s ISVS, přičemž pro řízení těchto informačních systémů bude krajský úřad používat stejné principy, metody a mechanismy jako pro ISVS.

### 1.2.2 Závaznost informační koncepce

Tato informační koncepce je závazná pro všechny organizační jednotky, zaměstnance, dodavatele a jiné uživatele informačního systému, jehož správcem je Olomoucký kraj.

Informační koncepce se týká existujících i nově pořizovaných a zaváděných částí informačního systému veřejné správy. Všechny ostatní směrnice a nařízení, které mají vztah k řízení kvality a bezpečnosti informací, jež jsou ve zmíněném informačním systému veřejné správy zpracovávány, jsou této informační koncepcí podřízeny.

### 1.2.3 Vazby informační koncepce

Tento dokument bere v úvahu prostředí, ve kterém krajský úřad působí, zejména zákony a právní předpisy vztahující se na činnost úřadu i další smluvní závazky.

**Informační koncepce** představuje dlouhodobou orientaci úřadu v oblasti informačních technologií, systémů, zdrojů a služeb. Vychází ze závěrů globální strategie krajského úřadu a navazuje na základní zásady popsané v dokumentu Rozvoj informační společnosti Olomouckého kraje.

Informační koncepce je otevřený dokument, který je upřesňován a doplňován podle změn, které se dějí jak uvnitř krajského úřadu samotného, tak v okolním světě, tak i v souvisejících obecně platných legislativních předpisech a normách.

### 1.2.4 Legislativní rámec informační koncepce

Informační koncepce se opírá zejména o níže uvedené zákony, vyhlášky a nařízení (uvedený seznam není úplným výčtem platné legislativy v této oblasti).

- Zákon č. 365/2000 Sb. o informačních systémech veřejné správy, v aktuálním znění,
- Vyhláška č. 528/2006 Sb. o informačním systému o ISVS,
- Vyhláška č. 529/2006 Sb. o dlouhodobém řízení ISVS,
- Vyhláška č. 530/2006 Sb. o postupech atestačních středisek,
- Vyhláška č. 469/2006 Sb. o informačním systému o datových prvcích,
- Vyhláška č. 53/2007 Sb. o referenčním rozhraní,
- Vyhláška č. 64/2008 Sb. o přístupnosti,
- Zákon č. 101/2000 Sb. o ochraně osobních údajů,
- Zákon č. 106/1999 Sb. o svobodném přístupu k informacím,
- Zákon č. 227/2005 Sb. o elektronickém podpisu,
- Nařízení vlády č. 304/2001 Sb., kterým se provádí zákon č.227/2000 Sb.,
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,
- Zákon č. 121/2000 Sb. autorský zákon,
- Zákon č. 129/2000 Sb. o krajích (krajské zřízení) a řada zákonů přiznávající kraji přenesenou působnost v oblasti výkonu státní správy.
- Zákon č. 499/2004 Sb. o archivnictví a spisové službě,
- Další zákony, například zákon č. 89/1995 Sb., o státní statistické službě, ve znění zákona č. 356/1999 Sb., zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů, zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů, zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.

## 1.3 Organizace dokumentu

### 1.3.1 Základní údaje

Tabulka č. 1: Základní údaje o informační koncepci

<b>Název organizace</b>	Olomoucký kraj
<b>IČO:</b>	60609460
<b>Typ organizace</b>	kraj
<b>Adresa:</b>	Jeremenkova 40a, 779 11 Olomouc
<b>Doba platnosti</b>	5 let
<b>Konec platnosti</b>	30. 11. 2019
<b>Aktuální verze</b>	2.0

Tabulka č. 2: Autorizace a schválení informační koncepce

Role	Osoba	Datum	Podpis
<b>Zpracovali:</b>	Mgr. Jiří Šafránek vedoucí odboru informačních technologií Krajský úřad Olomouckého kraje <a href="mailto:j.safranek@kr-olomoucky.cz">j.safranek@kr-olomoucky.cz</a>	30. 11. 2014	
	Ing. Ivan Russnák odbor informačních technologií Krajský úřad Olomouckého kraje <a href="mailto:i.russnak@kr-olomoucky.cz">i.russnak@kr-olomoucky.cz</a>		
<b>Schválil:</b>	Mgr. Lucie Štěpánková Ředitel Krajský úřad Olomouckého kraje <a href="mailto:reditel@kr-olomoucky.cz">reditel@kr-olomoucky.cz</a>	15.1.2016	

Verze informační koncepce jsou číslovány vzestupně od 1.0, přičemž v dalších odstavcích jsou uvedeny základní údaje o aktuálně platné verzi i o verzích předešlých vždy s vyznačením změn oproti předešlé verzi.

### 1.3.2 Verze 2.0 - aktuální verze informační koncepce

Tabulka č. 3: Údaje o verzi 2.0 informační koncepce

<b>Verze:</b>	2.0
<b>Status:</b>	schváleno
<b>Platnost od:</b>	1. 12. 2014
<b>Zpracovali:</b>	Mgr. Jiří Šafránek, vedoucí odboru informačních technologií <a href="mailto:j.safranek@kr-olomoucky.cz">j.safranek@kr-olomoucky.cz</a> Ing. Ivan Russnák

Schválil:	Mgr. Lucie Štěpánková, ředitelka Krajského úřadu Olomouckého kraje
Vytvořeno dne:	30. 11. 2014
Schváleno dne:	16.9.2015
Počet stran:	41
Počet příloh:	4
Umístění:	Intranet – soubor: informační koncepce 2.0

Tabulka č. 4: Změny provedené ve verzi 2.0 oproti verzi 1.2

Identifikace změněné části	Popis a odůvodnění změny
Přidána příloha	Příloha č. 2 Katalog informačních systémů
Přidána příloha	Příloha č. 3 Plán rozvoje informačních systémů
Přidána příloha	Příloha č. 4 Plán financování informačních systémů

### 1.3.3 Verze 1.2

Tabulka č. 5: Údaje o verzi 1.2 informační koncepce

Verze:	1.2
Status:	schváleno
Platnost od:	1. 10. 2012
Zpracovali:	Mgr. Jiří Šafránek, vedoucí odboru informačních technologií <a href="mailto:j.safranek@kr-olomoucky.cz">j.safranek@kr-olomoucky.cz</a> Ing. Ivan Russnák
Schválil:	JUDr. mag. iur. Michal Malacka, PhD., MBA, ředitel Krajského úřadu Olomouckého kraje
Vytvořeno dne:	30. 09. 2012
Schváleno dne:	30. 09. 2012
Počet stran:	8441
Počet příloh:	0
Umístění:	Intranet – soubor: Informační koncepce 1.2

Tabulka č. 6: Změny provedené ve verzi 1.2 oproti verzi 1.1

Identifikace změněné části	Popis a odůvodnění změny
Revize verze 1.1	Revize seznamu obhospodařovaných ISVS, revize dlouhodobých cílů v oblasti řízení kvality ISVS

### 1.3.4 Verze 1.1

Tabulka č. 7: Údaje o verzi 1.1 informační koncepce

Verze:	1.1
Status:	schváleno
Platnost od:	1. 7. 2012
Zpracovali:	Mgr. Jiří Šafránek, vedoucí odboru informačních technologií <a href="mailto:j.safranek@kr-olomoucky.cz">j.safranek@kr-olomoucky.cz</a>
Schválil:	Bc. Ing. Libor Kolář, ředitel Krajského úřadu Olomouckého kraje
Vytvořeno dne:	30. 06. 2012
Schváleno dne:	30. 06. 2012
Počet stran:	7441
Počet příloh:	0
Umístění:	Intranet – soubor: Informační koncepce 1.1

Tabulka č. 8: Změny provedené ve verzi 1.1 oproti verzi 1.0

Identifikace změněné části	Popis a odůvodnění změny
Revize verze 1.0	Úprava seznamu obhospodařovaných ISVS, úprava dlouhodobých cílů v oblasti řízení kvality ISVS

### 1.3.5 Verze 1.0 - výchozí verze informační koncepce

Tabulka č. 9: Výchozí verze informační koncepce

Verze:	1.0
Status:	schváleno
Platnost od:	3. 12. 2009
Zpracovali:	Mgr. Jiří Šafránek, vedoucí odboru informačních technologií <a href="mailto:j.safranek@kr-olomoucky.cz">j.safranek@kr-olomoucky.cz</a> Ing. Mgr. Marek Solařík, TNS, a.s., <a href="mailto:marek.solarik@tns.cz">marek.solarik@tns.cz</a>
Schválil:	Bc. Ing. Libor Kolář, ředitel Krajského úřadu Olomouckého kraje
Vytvořeno dne:	27. 8. 2009
Schváleno dne:	3. 12. 2009
Počet stran:	5041
Počet příloh:	2
Umístění:	Intranet – soubor: KUOL-prj02-Infornační koncepce-20090810-001.pdf



### 1.3.6 Struktura dokumentu

Z pohledu zákona č. 365/2000 Sb. (dále též jen Zákon) reprezentuje tento dokument zejména paragraf 5a - Dlouhodobé řízení informačních systémů veřejné správy, odstavec 1. Dokument je dále členěn na jednotlivé kapitoly v souladu s vyhláškou č. 529/2006 Sb. (dále též jen Vyhláška).

**Kapitola 1** definuje předmět a účel informační koncepce, definuje rozsah, závaznost a vazby, uvádí informace o verzích a dobu platnosti informační koncepce v souladu s § 2, odstavec 1, písmeno i Vyhlášky.

**Kapitola 2** vypočítává informační systémy ve správě krajského úřadu. Podrobnější informace o jednotlivých informačních systémech jsou uvedeny dále v příloze č. 1 v souladu s § 2, odstavec 1, písmeno a Vyhlášky.

**Kapitola 3** uvádí záměry na pořízení nebo vytvoření nových informačních systémů veřejné správy v souladu s § 2, odstavec 1, písmeno b Vyhlášky.

**Kapitola 4** definuje dlouhodobé cíle krajského úřadu v oblasti řízení kvality ISVS a uvádí plán řízení kvality. Odpovídá požadavkům § 2, odstavec 1, písmeno c a požadavkům § 3 Vyhlášky.

**Kapitola 5** definuje dlouhodobé cíle krajského úřadu v oblasti řízení bezpečnosti ISVS a uvádí plán řízení bezpečnosti. Odpovídá požadavkům § 2, odstavec 1, písmeno d a požadavkům § 4 Vyhlášky.

**Kapitola 6** stanovuje zásady a postupy pro správu ISVS v souladu s § 2, odstavec 1, písmeno e Vyhlášky. Tyto zásady a postupy jsou uvedeny zvlášť pro pořizování a vytváření ISVS a zvlášť pro provozování ISVS v souladu s § 2, odstavec 3 a v souladu s § 8 resp. § 9 Vyhlášky.

**Kapitola 7** popisuje způsob financování rozvoje a správy ISVS v souladu s § 2, odstavec 1, písmeno f Vyhlášky.

**Kapitola 8** definuje kontrolní mechanismy a postupy pro vyhodnocování informační koncepce a postupy pro její schvalování a úpravy v souladu s § 2, odstavec 1, písmeno g, § 6 a § 7 Vyhlášky.

**Kapitola 9** definuje organizační strukturu pro řízení kvality a bezpečnosti ISVS, definuje povinnosti a odpovědnosti zúčastněných osob v souladu s § 2, odstavec 1, písmeno h Vyhlášky.

**Kapitola 10 - Příloha 1** obsahuje podrobný popis jednotlivých informačních systémů, jejichž správcem je krajský úřad Olomouckého kraje.

## 1.4 Přehled zkratk

IT	informační technologie
ICT	informační a komunikační technologie
IS	informační systém
ISVS	informační systém veřejné správy
PIS	provozní informační systém

OVS	orgán veřejné správy
KÚOK	Krajský úřad Olomouckého kraje
PO	příspěvková organizace
ORP	obec s rozšířenou působností
TC	technologické centrum
TC_K	technologické centrum na úrovni kraje
TC_ORP	technologické centrum na úrovni ORP
HW	hardware
SW	software
WAN	wide area network
LAN	local area network
GIS	grafický informační systém
DMS	document management system
PDCA	Plan Do Check Act
AAA	Authentization Authorization Accounting
V/V	Vstup / Výstup
DRP	Disaster Recovery Plan
NNO	nestátní nezisková organizace

## 2 Popis ISVS

Informační systém veřejné správy, jehož správcem je Olomoucký kraj, je tvořen několika samostatnými informačními systémy, jež jsou přehledně uvedeny v následující tabulce a podrobně pak popsány v příloze č. 1.

V tabulce jsou pro přehlednost uvedeny pouze informační systémy veřejné, které slouží k výkonu veřejné správy a tvoří tak **informační systém veřejné správy (ISVS)**. Kromě toho jsou na úřadu provozovány další informační systémy, které slouží pro podporu vnitřních činností úřadu – tzv. provozní informační systémy (PIS) a informační pro podporu informačních systémů – tzv. podpůrné informační systémy (PoIS).

Tabulka č. 10: Přehled informačních systémů veřejné správy

ID	Název (dodavatel)	Typ	Specifikace
IS 1	<b>Clix-registr oznámení</b> (BMI SYSTEM CZECH, a.s.)	ISVS	Registr oznámení dle 159/2006 Sb., o střetu zájmů
IS 2	<b>CzechPoint</b> (MV ČR)	ISVS	český podací a ověřovací národní terminál
IS 3	<b>ESPI - Evidence správních řízení, EVI - Evidence odpadů, zařízení</b> (Inisoft s.r.o.)	ISVS	ESPI - evidence a tvorba rozhodnutí o nakládání s odpady, data jsou automaticky exportována na náš www server EVI - data z obcí Evidence rozhodnutí, synchronizace dat vykázaných obcemi III. stupně
IS 4	<b>Evidence dopravních agend</b> (YAMACO Software)	ISVS	komplexní informační systém pro agendy odborů dopravy ve státní a veřejné správě
IS 5	<b>Evidence myslivosti</b> (YAMACO Software)	ISVS	importujeme data z obcí a předáváme data na MZE ČR + komunikace s Dotace LH+
IS 6	<b>Evidence správních agend</b> (IS MVCR)	ISVS	registr obyvatel, státní občanství ČR
IS 7	<b>Evidence středních a malých zdrojů (OvzdušSQL)</b> (Kvasar)	ISVS	export z programu pro státní fond životního prostředí cca jednou měsíčně probíhá téměř automaticky po odsouhlasení uživatele pravděpodobně www služba možnost exportů z programu (roční výkaz; export pro ČHMÚ) - e-mailem, v současné době se předávání dat neuskutečňuje, je plánováno v budoucnosti
IS 8	<b>eVPE (Editor vodoprávní evidence)</b> (Ministerstvo zemědělství ČR)	ISVS	export dat na MZE ČR pomocí web služeb
IS 9	<b>iLAS + IKAS</b> (MMR ČR)	ISVS	pasport územních plánů velkých územních celků a obcí (webová aplikace provozovaná

ID	Název (dodavatel)	Typ	Specifikace
			centrálně)
IS 10	<b>ISP</b> (kraj)	ISVS	automatické zpracování souborů do Informačního Systému o Platech
IS 11	<b>ISPROFIN</b> (SYSCOM SOFTWARE spol. s r.o.)	ISVS	program SFDI - čtvrtletně zasíláno na SFDI - e-mailem
IS 12	<b>MPSV sumarizace</b>	ISVS	sociální zařízení nám posílají vyplněné formuláře, které v programu sumarizujeme a posíláme na MPSV (SW pro sumarizaci dat MPSV)
IS 13	<b>Informační systém GINIS</b> (GORDIC, s.r.o.)	ISVS	modul elektronické podatelny systému elektronické spisové služby, spisová služba KÚ, sumarizační modul rozpočtu a účetnictví
IS 14	<b>Účetnictví a rozpočet (GorUCR)</b> (GORDIC, s.r.o.)	ISVS	file systém - sběr účetních dat obcí
IS 15	<b>Úřední deska</b> (kraj)	ISVS	intranetová aplikace
IS 16	<b>Územně identifikační registr (UIR-ADR)</b> (Ministerstvo práce a sociálních věcí)	ISVS	územně identifikační registr adres
IS 17	<b>Výkaznictví (GorVYK)</b> (GORDIC, s.r.o.)	ISVS	náklady společné s GorUCR příspěvkové organizace zasílají data (výkazy) na e-mail, kde je automaticky program kontroluje a načítá.

## 3 Záměry na pořízení nebo vytvoření nových IS

### 3.1 Plán rozvoje IS

Záměry na pořízení nebo vytvoření nových IS jsou uvedeny v Plánu rozvoje ISVS, který obsahuje následující části:

- plán pořizování a vytváření nových IS,
- plán provozování a údržby provozovaných IS,
- plán provádění změn stávajících IS,
- plán ukončení činnosti IS.

Plán rozvoje ISVS obsahuje též harmonogram provádění jednotlivých akcí.

**Plán** zpracovává pověřený pracovník odboru informačních technologií a ke schválení vedení kraje předkládá vedoucí odboru informačních technologií. Aktualizace plánu, jeho kontrola a schvalování se provádí **v roční periodicitě**.

Krajský úřad Olomouckého kraje bude v následujících obdobích postupně rozšiřovat možnosti svých IS o propojení na centrální registry přes referenční rozhraní, která budou definována příslušnými správci centrálních IS.

Rovněž budou probíhat úpravy stávajících IS tak, aby informace v nich zpracovávané mohly být diferencovaně dostupné širokému spektru adresátů a to nejen zaměstnancům Krajského úřadu a představitelům Olomouckého kraje, zaměstnancům a představitelům OVS, nadřízeným či spolupracujícím veřejným orgánům, ale i komerčním subjektům na komerčním základě. Budou též probíhat úpravy propojení stávajících IS tak, aby jednou pořízené informace a data nemusely být vkládány znovu, ale byly opakovaně využívány.

Další plánovanou změnou stávajících IS je rozšíření funkcionality vlastních IS a jejich vzájemné propojení pro efektivní – tj. automatický – sběr informací o všech aktivech (majetek, finance, hodnoty) Olomouckého kraje, příspěvkových organizací a olomouckého regionu.

Nově plánuje Olomoucký kraj pořídit IS digitální mapa a IS pro podporu konverze dokumentů a digitalizace, ukládání a archivace dat.

Všechny úpravy a změny stávajících IS a pořizování nových IS musí být prováděny dle zásad definovaných v kapitole 6.

Kromě výše popsaných změn jsou plánovány též činnosti související s údržbou a se zvyšováním kvality a posílením bezpečnosti dat a služeb zpracovávaných a poskytovaných IS Olomouckého kraje. Tyto činnosti jsou podrobně popsány v kapitolách 4 a 5.

## 4 Řízení kvality IS

### 4.1 Účel IS

#### 4.1.1 Základní principy

Dlouhodobé cíle v oblasti řízení kvality a bezpečnosti IS vycházejí ze základních principů veřejné správy, kterými jsou:

1. **Důsledné dodržování práva, spolehlivost a předvídatelnost** – každé jednání musí být podepřeno právní jistotou, nestranností a profesní nezávislostí.
2. **Otevřenost a transparentnost** (jednání, rozhodování, hospodaření s veřejnými prostředky) – musí být zajištěna možnost kontroly, povinnost zdůvodňovat svá rozhodnutí, zveřejňovat základní informace o svých činnostech i umožnit přístup k informacím.
3. **Odpovědnost** – každý orgán veřejné správy se musí zodpovídat ze své činnosti jinému orgánu a veřejnosti a musí podléhat různým formám dohledu.
4. **Účinnost (efektivnost)** – musí být udržován přijatelný poměr mezi použitými zdroji a dosaženými výsledky, úspěšnost v řešení problémů a dosahování cílů. Hlavní je přitom tzv. vnější efektivnost, tj. působení veřejné správy směrem do společnosti (plnění společenské úlohy veřejné správy).
5. **Dodržování zásady rovnosti, nestrannosti a ochrana před zneužitím** – všechny zákony a nařízení by měly být navrhovány a uplatňovány tak, aby byly neutrální a obecně platné, a aby nemohlo dojít k jejich zneužití či k formám nespravedlnosti vůči vybraným fyzickým i právnickým osobám.

Výše uvedené principy definují rámec pro budování, užívání a správu IS. Z tohoto pohledu lze chápat:

#### 4.1.2 IS jako nástroj

- **zefektivnění výkonu veřejné správy** – výrazný důraz je kladen na optimalizaci a automatizaci úředních procesů.
- **podpory transparentnosti veřejné správy** – volný a rovný přístup k informacím o činnosti orgánů veřejné správy s důrazem na jejich dostupnost
- **zviditelnění Olomouckého kraje (územně správního celku)** – IT jsou jedním z mnoha nástrojů, které umožňují efektivní prezentaci regionu a podporu soudržnosti regionu.
- **podpory rozvoje Olomouckého kraje (územně správního celku)** -odvětví informačních a komunikačních technologií, kam spadají i IS, je kromě nástroje podporujícího regionální rozvoj také významným, dynamicky se rozvíjejícím sektorem ekonomiky.

### 4.1.3 IS jako služba

- **veřejnosti** – IS musí sloužit veřejnosti k efektivní komunikaci s veřejnou správou. IS musí být v tomto směru doopravdy službou, nikoliv překážkou.
- **managementu veřejné správy** – včasný přísun kvalitních informací a nástroje pro jejich zpracování a vyhodnocování jsou nezbytné pro kvalitní řízení nejen samosprávných orgánů.
- **zaměstnancům orgánů veřejné správy** – se vzrůstajícími nároky na kvalitu výkonu úředníků je zvládnutí a využití nástrojů ICT prakticky nutnou podmínkou. I v této oblasti musí být informatika službou, nikoliv překážkou či cílem. Významnou cílovou skupinou jsou vedle zaměstnanců krajského úřadu také krajem zřizované organizace.

## 4.2 Dlouhodobé cíle v oblasti řízení kvality IS

Dlouhodobé cíle v oblasti řízení kvality IS vycházejí z výše uvedených základních principů a cílů pro informační systém veřejné správy. V souladu s § 3 vyhlášky č. 529/2006 Sb. jsou dlouhodobé cíle stanoveny ve třech následujících oblastech:

- zajištění **kvality dat**, která jsou v IS zpracovávána,
- zajištění **kvality technických a programových prostředků IS**,
- zajištění **kvality služeb**, které jsou prostřednictvím IS poskytovány.

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

Tabulka č. 11: Dlouhodobé cíle v oblasti řízení kvality IS

Oblast kvality	Označení cíle	Název cíle	Popis cíle	Atribut kvality
Kvalita dat	CK-1	<b>Kvalitní data</b>	<b>Integrita, validita, odpovědnost</b> Data zpracovávána v IS bez duplicit, odpovídající realitě, data správná a přesná. Vazba na centrální registry.	Bezporuchovost, Funkčnost
	CK-2	<b>Digitální mapa</b>	Zajištění digitálních mapových podkladů a jejich údržba.	Funkčnost Použitelnost
	CK-3	<b>Digitální data</b>	Zajištění procesu digitalizace současných dokumentů a podkladů a jejich archivace.	Udržitelnost Funkčnost Použitelnost
Kvalita služeb	CK-4	<b>Přístupný úřad</b>	Rozšíření a zjednodušení komunikace občanů s úřadem, průběžné zkvalitňování dostupných rozhraní úřad – občan/podnikatel/OVS, v souladu s požadavky projektů eGovernment.	Použitelnost
	CK-5	<b>Dostupná data</b>	Vytvoření centrálního datového skladu s výstupy pro celé území kraje.	Použitelnost

Oblast kvality	Označení cíle	Název cíle	Popis cíle	Atribut kvality
	CK-6	<b>Správa aktiv</b>	Efektivní sběr a prezentace dat o aktivech (majetek, finance, hodnoty) Olomouckého kraje, organizací zřizovaných Olomouckého kraje, Olomouckého regionu s cílem poskytnout spolehlivou platformu pro vrcholové rozhodování.	Funkčnost Použitelnost
	CK-7	<b>Výkonný úřad</b>	<b>Integrace chodu úřadu</b> Podpora provádění všech činností a agend úřadu, popisy procesů, jejich automatizace, integrace vnitřních i komunikujících informačních systémů.	Účinnost
	CK-8	<b>Integrovaná veřejná správa</b>	<b>Spolupráce</b> v rámci regionu s obcemi s rozšířenou působností, příspěvkovými organizacemi a komerční sférou, poskytnutí služeb IS i těmto subjektům.	Funkčnost
<b>Kvalita technických a programových prostředků</b>	CK-9	<b>Technologické centrum</b>	Provoz technologického centra (HW, SW, infrastruktura) na krajské úrovni pro zajištění služeb pro zaměstnance KÚOK, PO i ostatních subjektů.	Funkčnost Použitelnost Bezporuchovost Udržovatelnost
	CK-10	<b>Páteří sít' Olomouckého kraje</b>	Vybudování páteří sítě veřejné správy Olomouckého kraje s cílem propojit TC_K a TC_ORP a zajistit tak plnohodnotné využití provozovaných služeb.	Funkčnost Použitelnost Bezporuchovost
	CK-11	<b>Integrace do prostředí ITS MV</b>	Vybudování optické hospoje do prostředí Integrované telekomunikační sítě MV	Funkčnost Použitelnost Bezporuchovost



### 4.3 Požadavky na kvalitu IS

Pro dosažení cílů stanovených v předchozím odstavci byly definovány požadavky na kvalitu, jež jsou přehledně uvedeny v následující tabulce. Zde je uveden též odkaz na cíl, ke kterému se daný požadavek váže a identifikace IS, pro který daný požadavek platí.

Tabulka č. 12: Požadavky na kvalitu IS

Cíl kvality	Označení požadavku	Název požadavku	Popis požadavku	Primární IS
CK-1 Kvalitní data	PK-1-01	<b>Aktuální data</b>	Data zpracovávaná v IS musejí odpovídat reálnému stavu, musejí být aktuální. Rovněž veškeré informace prezentované IS musí být aktuální a odpovídat realitě.	Všechny IS
	PK-1-02	<b>Správná data</b>	V IS musejí být dostupná všechna data, která jsou pro výkon státní správy a samosprávy nezbytná. Zároveň IS ani žádná jeho část nesmí obsahovat data, která pro výkon státní správy a samosprávy nezbytná nejsou.	Všechny IS
	PK-1-03	<b>Konzistentní data</b>	V jednotlivých IS a jejich databázích musí být zajištěna integrita dat, musí být vyloučena duplicita apod. Totéž je požadováno i napříč celým IS.	Všechny IS
	PK-1-04	<b>Využití centrálních registrů</b>	IS musejí být navrhovány, implementovány a spravovány tak, aby v co možná největší míře využívaly dat centrálních registrů (resp. tuto možnost předem obsahovaly).	Všechny IS
CK-2 Digitální mapa	PK-2-01	<b>Digitální mapa</b>	Mapové podklady musejí být dostupné všem oprávněným uživatelům v digitální podobě.	GIS
	PK-2-02	<b>Aktualizace mapových podkladů</b>	Mapové podklady musí být udržovány aktuální, automatické aktualizace musí být prováděny podle plánu aktualizace u jednotlivých kategorií.	GIS
	PK-2-03	<b>Srozumitelné výstupy</b>	Mapové podklady musí umožnit prezentaci různých přehledů, statistik, agend zpracovávaných úřadem, návrhů a rozhodnutí týkajících se území Olomouckého kraje apod. a to přehledným způsobem pro všechny občany kraje.	GIS
CK-3 Digitální data	PK-3-01	<b>Digitalizace dat</b>	Veškeré dokumenty a podklady musejí být dostupné v digitální podobě. Důraz je kladen na snadné vyhledávání dokumentů a podkladů a na snadné prohledávání jejich obsahu.	DMS
	PK-3-02	<b>Konverze dokumentů</b>	Musejí být zavedeny postupy pro snadný převod klasických tištěných dokumentů a podkladů do digitální podoby a též pro převod opačný.	DMS

CK-4 Přístupný úřad	PK-4-01	<b>Vše potřebné na jednom místě</b>	Veškeré informace, formuláře, návody na postup pro řešení různých životních situací, vyhlášky, rozhodnutí, kontakty apod. musejí být dostupné přes jednotné rozhraní IS.	Web
	PK-4-02	<b>Přehlednost informací</b>	Veškeré informace atd. (viz výše) musejí být přehledně uspořádány, musí být možné je snadno nalézt, musí být přístupné nástroje pro strojové vyhledávání.	Web
	PK-4-03	<b>Snadno použitelné nástroje</b>	Je kladen důraz na jednoduchost a snadnou použitelnost nástrojů a funkcí IS i pro občany detailně neznalé konkrétní problematiky, občany starší a tělesně postižené.	Web
CK-5 Dostupná data	PK-5-01	<b>Obsahová dostupnost dat</b>	Data musejí být dostupná přes jednotné rozhraní oprávněným uživatelům – a to jak vnitřním, tak zejména uživatelům z PO, firem z regionu, jiným správním orgánům i široké veřejnosti - za předem stanovených a kontrolovaných podmínek.	Web, WAN
	PK-5-02	<b>Časová dostupnost dat</b>	Data (viz výše) musejí být dostupná v režimu 24x7. V běžném provozu nesmí nedostupnost přesáhnout 1 den, v krizové situaci musejí být potřebná data dostupná oprávněným uživatelům do 4 hodin.	Web, WAN
CK-6 Správa aktiv	PK-6-01	<b>Efektivní sběr informací</b>	Data o všech aktivech (majetek, finance, hodnoty) Olomouckého kraje, příspěvkových organizací a olomouckého regionu musejí být udržován aktuální automatickým způsobem.	Všechny IS
	PK-6-02	<b>Přehledná prezentace</b>	Báze dat o aktivech musí umožňovat snadno vytvářet přehledné výstupy pro různé skupiny oprávněných uživatelů.	Web, WAN
CK-7 Výkonný úřad	PK-7-01	<b>Procesní mapa</b>	Všechny činnosti úřadu musejí být přehledně zobrazeny včetně případných vzájemných závislostí, odkazů na příslušné odbory a zodpovědné pracovníky a informační nástroje a zdroje.	Všechny IS
	PK-7-02	<b>Účinné nástroje</b>	Všechny IS Úřadu musejí být navrhovány a pořizovány s ohledem na snadné ovládání, snadné použití vstupů z jiných IS a snadnou úpravu a použití výstupů v návazných IS.	Všechny IS
CK-8 Integrovaná veřejná správa	PK-8-01	<b>Přístupné IS</b>	Všechny IS musejí poskytovat různé typy přístupů na základě autentizace a autorizace konkrétního uživatele či druhého systému a to všem uživatelům – nejen vnitřním, ale zvláště dalším OVS, komerčním i nekomerčním subjektům a občanům olomouckého regionu.	Všechny IS

	PK-8-02	<b>Kooperující IS</b>	Jednotlivé IS musejí být vzájemně propojeny tak, aby jednou pořízené či zpracované údaje bylo možné ihned snadno použít při dalším zpracovávání.	Všechny IS
	PK-8-03	<b>Externí využití</b>	Všechny IS musejí být navrhovány, pořizovány a provozovány s ohledem na možnost nabídnout služby těchto IS dalším subjektům na nekomerční i komerční bázi.	Všechny IS
CK-9 Technologické centrum	PK-9-01	<b>Kvalitní prostředí a služby</b>	Technologické centrum musí být schopno nabízet kvalitní základní služby (telekomunikace, napájení, klimatizace, fyzická a požární ochrana) i rozšiřující služby (zálohování, ochrana telekomunikačního provozu apod.) pro provoz aplikací a systémů jak vlastních, tak cizích, na nekomerčním i komerčním základě.	Dotčené IS
CK-10 Pátevní síť Olomouckého kraje	PK-10-01	<b>Jednotná infrastruktura</b>	Moderní a technologicky jednotná pátevní síť s malou poruchovostí.	WAN
	PK-10-02	<b>Vysoká kapacita</b>	Dostatečně dimenzovaná kapacita pátevní sítě s ohledem na potřeby celého Olomouckého kraje.	WAN
	PK-10-03	<b>Snadná rozšiřitelnost</b>	Snadno rozšiřitelná síť jak z pohledu kapacity, tak z pohledu počtu zapojených subjektů.	WAN
	PK-10-04	<b>Jednotná správa</b>	Jednotná správa s definovanými postupy a vstupními i výstupními rozhraními vůči zapojeným subjektům.	WAN

#### 4.4 Plán řízení kvality IS

Činnosti, které krajský úřad provádí k dosažení stanovených požadavků na kvalitu IS a které jsou společně s činnostmi prováděnými k dosažení požadavků na bezpečnost IS, jsou uvedeny souhrnně v kapitole 9.

V následující tabulce jsou uvedeny činnosti k dosažení požadavků na kvalitu popsaných v odstavci 4.3, přičemž je uveden i časový harmonogram jejich plnění.

Tabulka č. 13: Plán řízení kvality IS

Označení požadavku	Název požadavku	Činnost	Popis činnosti	zahájení	ukončení	Poznámka
PK-1-01	aktuální data	K-1	Stanovení zodpovědnosti za data	12/2014	06/2015	
		K-2	Implementace vstupních kontrol	12/2014	12/2015	

		<b>K-3</b>	Implementace výstupních kontrol	12/2014	12/2015	
		<b>K-4</b>	Počáteční audit a konsolidace dat	10/2014	05/2015	
		<b>K-5</b>	Opakovaný audit a konsolidace dat, vyhodnocení, úpravy	10/každý rok	11/ každý rok	
PK-1-02	správná data	<b>K-4</b>	Počáteční audit a konsolidace dat	12/2014	06/2015	společně s PK-1-01
		<b>K-2</b>	Implementace vstupních kontrol	12/2014	12/2015	společně s PK-1-01
		<b>K-3</b>	Implementace výstupních kontrol	12/2014	12/2015	společně s PK-1-01
		<b>K-5</b>	Opakovaný audit a konsolidace dat, vyhodnocení, úpravy	10/každý rok	11/ každý rok	od r. 2016
PK-1-03	konzistentní data	<b>K-4</b>	Počáteční audit a konsolidace dat	12/2014	06/2015	společně s PK-1-01
		<b>K-2</b>	Implementace vstupních kontrol	12/2014	12/2015	společně s PK-1-01
		<b>K-3</b>	Implementace výstupních kontrol	12/2014	12/2015	společně s PK-1-01
		<b>K-5</b>	Opakovaný audit a konsolidace dat, vyhodnocení, úpravy	10/každý rok	11/ každý rok	od r. 2016
PK-2-01	Digitální mapa	<b>K-6</b>	Identifikace klíčových uživatelů a jejich požadavků.	10/2012	12/2019	Aktualizováno průběžně
		<b>K-7</b>	Zajištění digitálních mapových podkladů, příslušného SW a HW dle zásad definovaných v kapitole 6.1.	12/2012	06/2019	Aktualizováno průběžně
PK-2-02	Aktualizace mapových podkladů	<b>K-8</b>	Vypracování plánu aktualizací.	04/2012	06/2012	Ukončeno
		<b>K-9</b>	Pravidelná aktualizace mapových podkladů.	Dle potřeby		
		<b>K-10</b>	Vyhodnocení aktualizací a revize plánu aktualizací pro další rok.	10/každý rok	10/každý rok	

PK-2-03	Srozumitelné výstupy	K-11	Audit výstupů vůči požadavkům a připomínkám klíčových uživatelů.	02/každý rok	02/každý rok	
PK-3-01	Digitalizace dat	K-12	Výběr, zavedení a provozování nového IS DMS dle zásad definovaných v kapitole 6.			
PK-3-02	Konverze dokumentů	K-13	Výběr, zavedení a provozování nového IS DMS dle zásad definovaných v kapitole 6.			
PK-4-01	vše potřebné na jednom místě	K-14	Stanovení zodpovědnosti za web	01/2015	03/2015	Web je převzat zpět do správy od externího dodavatele
		K-15	Implementace sledování návštěvnosti stránek – využívání informací	01/2015	01/2016	
		K-16	Vyhodnocení úplnosti informací - počáteční audit webu	01/2015	02/2015	
		K-17	opakovaný audit webu	06/2015	07/2015	
PK-4-02	přehlednost informací	K-18	Vyhodnocení přehlednosti webu - Anketa „Přehlednost webu“	12/2015	02/2016	
		K-19	opakovaný audit webu	01/2016	Ročně	
PK-4-03	snadno použitelné nástroje	K-20	Vyhodnocení přístupnosti webu - počáteční audit webu	01/2015	03/2015	
		K-21	opakovaný audit webu	01/2016	Ročně	
PK-5-01	nová dostupnost	K-22	Identifikace a klasifikace dat, uživatelů a přístupů.	05/2015	06/2015	

		<b>K-23</b>	Výběr, zavedení a provozování systému dle zásad definovaných v kapitole 6	08/2015	12/2019	Aktualizováno průběžně
		<b>K-24</b>	Audit systému.	05/každý lichý rok	05/každý lichý rok	
PK-5-02	Časová dostupnost dat	<b>K-25</b>	Implementace automatického sledování dostupnosti a eskalačních procedur.	06/2014	10/2014	
PK-6-01	Efektivní sběr informací	<b>K-26</b>	Provázání jednotlivých IS, definice a implementace kontrol.	10/2014	12/2019	Sběr informací na portále PO a portále majetku
		<b>K-27</b>	Hodnocení efektivity a dostupnosti informací o aktivech kraje.	05/každý rok	05/každý rok	
PK-6-02	Přehledná prezentace	<b>K-28</b>	Hodnocení snadnosti vytváření výstupů o aktivech kraje a jejich přehlednosti.	05/každý sudý rok	05/každý sudý rok	
PK-7-01	Procesní mapa	<b>K-29</b>	Vytvoření mapy procesů.	06/2016	09/2016	V minulém období nebyl projekt zahájen
PK-7-02	Účinné nástroje	<b>K-30</b>	Vytvoření topologie datových toků a komunikační mapy a zavedení procesů pravidelné aktualizace těchto informací.	10/2016	12/2016	
PK-8-01	Přístupné IS	<b>K-31</b>	Viz činnosti <b>K-22</b> až <b>K-26</b> popsané výše.			
PK-8-02	Kooperující IS	<b>K-32</b>	Vše řešeno podle zásad definovaných v kapitole 6.			

PK-8-03	Externí využití	K-33				
PK-9-01	Kvalitní prostředí a služby	K-34	Samostatný projekt Technologického centra kraje dle zásad definovaných v kapitole 6.			
PK-10-01	Jednotná infrastruktura	K-35	Samostatný projekt páteřní sítě Olomouckého kraje dle zásad definovaných v kapitole 6.			V minulém období nebyl projekt zahájen
PK-10-02	Vysoká kapacita					
PK-10-03	Snadná rozšiřitelnost					
PK-10-04	Jednotná správa					

## 5 Řízení bezpečnosti IS

### 5.1 Základní principy

Bezpečnost je nedílnou součástí IS spravovaných krajským úřadem Olomouckého kraje a je neoddelitelná od všech procesů, které zajišťují elektronickou datovou komunikaci a elektronické pořizování a zpracování dat. Ohled na bezpečnost musí být pevným závazkem každého pracovníka, který nakládá s informacemi v IS a využívá jeho služby.

Zajištění bezpečnosti IS znamená zajištění **důvěrnosti**, **integrity**, **dostupnosti** a **nepopiratelnosti** všech dat, technických a programových prostředků, služeb a činností, které jsou prostřednictvím IS prováděny.

## 5.2 Dlouhodobé cíle v oblasti řízení bezpečnosti IS

Dlouhodobé cíle v oblasti řízení bezpečnosti IS byly v souladu s § 4 vyhlášky č. 529/2006 Sb. stanoveny ve třech následujících oblastech:

- zajištění **bezpečnosti dat**, která jsou v IS zpracovávána,
- zajištění **bezpečnosti technických a programových prostředků IS**,
- zajištění **bezpečnosti služeb**, které jsou prostřednictvím IS poskytovány.

Dlouhodobé cíle v oblasti řízení bezpečnosti IS jsou uvedeny v následující tabulce, a to v členění do tří výše uvedených oblastí. U každého cíle je dále uveden atribut bezpečnosti, kterého sedaná cíl týká.

Tabulka č. 14: Dlouhodobé cíle v oblasti řízení bezpečnosti IS

Oblast bezpečnosti	Označení cíle	Název cíle	Popis cíle	Atribut bezpečnosti
Bezpečnost dat	CB-1	<b>Jednotná ochrana dat</b>	Definovaný a kontrolovaný přístup k datům zpracovávaných v IS a k jejich modifikaci.	Důvěrnost Integrita Nepopiratelnost
Bezpečnost služeb	CB-2	<b>Dostupné služby</b>	Služby poskytované prostřednictvím IS dostupné oprávněným uživatelům tehdy, kdy to potřebují.	Dostupnost
	CB-3	<b>Bezpečná rozhraní</b>	Zajištění bezpečnosti služeb – zejména vstupních rozhraní.	Integrita
Bezpečnost technických a programových prostředků	CB-4	<b>Technologické centrum</b>	Provoz krajského technologického centra jako bezpečného prostředí pro provoz vlastních aplikací i aplikací zřízených organizací a aplikací třetích stran.	Dostupnost
	CB-5	<b>Bezpečná správa</b>	Posílení monitoringu infrastruktury, logování, uchovávání a vyhodnocování auditních záznamů. Vypracování provozní dokumentace.	Nepopiratelnost Dostupnost Důvěrnost Integrita

## 5.3 Požadavky na bezpečnost IS

Pro dosažení cílů stanovených v předchozím odstavci byly definovány požadavky na bezpečnost, jež jsou přehledně uvedeny v následující tabulce. Zde je uveden též odkaz na cíl, ke kterému se daný požadavek váže a identifikace IS, pro který daný požadavek platí.

Tabulka č. 15: Požadavky na bezpečnost IS

Cíl bezpečnosti	Označení požadavku	Název požadavku	Popis požadavku	Primární IS



CB-1 Jednotná ochrana dat	PB-1-01	<b>Definovaný přístup k datům</b>	Jakýkoliv přístup k citlivým datům zpracovávaných v IS může být uskutečněn jen na základě jednoznačné autentizace a autorizace. Každý přístup a manipulace s těmito daty musí být zaznamenány.	všechny IS
	PB-1-02	<b>Zálohovaná data</b>	Data zpracovávaná v IS musejí být zálohována dle plánu záloh.	všechny IS
	PB-1-03	<b>Archivovaná data</b>	Data dlouhodobě archivovaná musejí být uchovávána na bezpečných nosičích mimo budovu úřadu bezpečným způsobem.	všechny IS
CB-2 Dostupné služby	PB-2-01	<b>Dostupnost služeb IS v běžném provozu</b>	Výpadek dostupnosti služeb poskytovaných IS nesmí v běžném provozu přesáhnout 1 den.	všechny IS
	PB-2-02	<b>Dostupnost služeb IS v krizové situaci</b>	V krizové situaci musejí být potřebné služby IS dostupné oprávněným uživatelům do 4hodin.	potřebné IS
CB-3 Bezpečná rozhraní	PB-3-01	<b>Kontrolované vstupy a výstupy</b>	Všechny vstupní a výstupní rozhraní musí zajišťovat kontrolu vstupních a výstupních údajů a zajišťovat ochranu před možnými útoky.	Web Všechny IS
CB-4 Technologické centrum	PB-4-01	<b>Projekt bezpečnosti Technologického centra</b>	Vlastnímu budování Technologického centra musí předcházet Projekt bezpečnosti, který podrobně definuje požadavky na bezpečnost vlastního centra a jeho služeb, požadavky na bezpečné propojení centra se stávajícími systémy Úřadu a požadavky na bezpečné provozování Technologického centra.	všechny IS
CB-5 Bezpečná správa	PB-5-01	<b>Provozní dokumentace</b>	Veškerá činnost správců i uživatelů musí být popsána v provozní dokumentaci IS.	všechny IS
	PB-5-02	<b>Monitoring</b>	Dostupnost a další výkonové parametry IS musejí být nepřetržitě automaticky monitorovány.	všechny IS
	PB-5-03	<b>Logování</b>	Veškeré činnosti uživatelů a správců IS musejí být automaticky zaznamenávány a vyhodnocovány. Auditní logy musejí být ukládány odděleně a s definovaným a kontrolovaným přístupem.	všechny IS
	PB-5-04	<b>Snadné zotavení po havárii</b>	IS musí být navržen a spravován tak, aby bylo snadné jeho obnovení po havárii. Obnovení kritických služeb musí být provedeno do 4 hodin, ostatních služeb do 1 dne.	všechny IS

## 5.4 Plán řízení bezpečnosti IS

Činnosti, které krajský úřad provádí k dosažení stanovených požadavků na bezpečnost IS a které jsou společné s činnostmi prováděnými k dosažení požadavků na kvalitu IS, jsou uvedeny souhrnně v kapitole 9.

V následující tabulce jsou uvedeny činnosti k dosažení požadavků na bezpečnost popsaných v odstavci 5.3, přičemž je uveden i časový harmonogram jejich plnění.

Tabulka č. 16: Plán řízení bezpečnosti IS

Označení požadavku	Název požadavku	Činnost	Popis činnosti	zahájení	ukončení	Poznámka
PB-1-01	Definovaný přístup k datům	B-1	Identifikace a klasifikace dat, uživatelů a přístupů.	05/2013	10/2013	společně s K-22
		B-2	Výběr, zavedení a provozování systému dle zásad definovaných v kapitole 6	05/2013	10/2013	společně s K-23
		B-3	Audit systému AAA.	05/každý lichý rok	05/každý lichý rok	společně s K-24
PB-1-02	Zálohovaná data	B-4	Výběr a implementace jednotného zálohování	05/2013	10/2013	Zálohování bylo převzato do správy kraje
		B-5	Test použitelnosti záloh	každý kvartál	každý kvartál	OIT
		B-6	Audit zálohování	10/každý sudý rok	11/každý sudý rok	
PB-1-03	Archivovaná data	B-7	Definice požadavků na archivaci	01/2015	10/2015	V rámci dodávky TC byl implementován nový způsob zálohování dat
		B-8	Definování a implementace procesu archivace	01/2015	10/2013	
		B-9	Test použitelnosti archivních dat	každý půlrok	každý půlrok	
		B-10	Audit archivace	10/každý sudý rok	11/každý sudý rok	
PB-2-01	služeb IS v běžném	B-11	Rozdělení kritických a nekritických částí IS	05/2013	10/2013	Ukončeno

		<b>B-12</b>	Konsolidace infrastruktury IS	06/2013	12/2013	Aktualizován o průběžně
		<b>B-13</b>	Návrh a implementace procesů správy IS	06/2015	12/2015	Budou implementovány nové služby (sběr dat pro ZS)
		<b>B-14</b>	Test dostupnosti	každý půlrok	Každý půlrok	
PB-2-02	Dostupnost služeb IS v krizové situaci	<b>B-15</b>	Návrh a implementace opatření k zajištění vysoké dostupnosti	06/2015	10/2015	Změny na základě zákona o kybernetické bezpečnosti
		<b>B-16</b>	Test dostupnosti	každý kvartál	každý kvartál	
PB-3-01	Kontrolované vstupy a výstupy	<b>B-17</b>	počáteční audit V/V rozhraní	05/2015	09/2015	
		<b>B-18</b>	Úprava V/V rozhraní	05/2015	12/2015	
		<b>B-19</b>	Externí penetrační test webu	05/2015	12/2015	
		<b>B-20</b>	opakovaný audit V/V rozhraní	05/2015	12/2015	
PB-4-01	Projekt bezpečnosti Technologického centra	<b>B-21</b>	Identifikace dotčených služeb, IS a klíčových uživatelů.	05/2015	12/2015	Požadavky zákona o KB
		<b>B-22</b>	Identifikace požadavků na bezpečnost.	05/2015	12/2015	
		<b>B-23</b>	Návrh bezpečnostních opatření.	12/2015	06/2016	
PB-5-01	Provozní dokumentace	<b>B-24</b>	Vypracování provozní dokumentace IS a nastavení procesů její aktualizace.	07/2015	12/2015	Významné změny provozní dokumentace v souvislosti s implementací nových technologií v TCK

PB-5-02	Monitoring	B-25	Zavedení jednotného monitoringu dostupnosti služeb IS a dalších výkonových parametrů a definice a zavedení eskalačních procedur.	07/2015	10/2015	
		B-26	Sledování výstupů monitoringu, reakce	průběžně	průběžně	Aktualizován o průběžně
PB-5-03	Logování	B-27	Zavedení jednotného logování činností uživatelů a správců	04/2015	10/2015	
		B-28	Vyhodnocení log záznamů	Každý kvartál	Každý kvartál	
PB-5-04	Snadné zotavení po havárii	B-29	Konsolidace infrastruktury IS	08/2013	11/2013	Ukončeno
		B-30	Vytvoření DRP plánů	09/každý rok	09/každý rok	Aktualizován o průběžně
		B-31	Testování DRP plánů	každý půlrok	každý půlrok	

## 6 Zásady a postupy pro správu IS

### 6.1 Zásady a postupy pro pořizování a vytváření IS

#### 6.1.1 Vytváření IS

Krajský úřad nebude žádné IS vlastními silami vytvářet, v případě potřeby nového IS se bude toto řešit formou dodávky od externího dodavatele dle zásad popsanych v následujícím odstavci.

#### 6.1.2 Pořizování IS

Pořizování nového IS se děje v níže uvedených krocích:

1. Záměr
2. Výběr
3. Implementace
4. Testovací provoz
5. Školení
6. Ostrý provoz

##### 6.1.2.1 Záměr

V úvodní fázi je definována potřeba nového IS, stanoveny funkční, kvalitativní a bezpečnostní požadavky, je uvedena analýza výchozího stavu a popsán stav cílový. Je též odhadnuta finanční, personální a časová náročnost a analyzovány dopady, které implementace nového IS vyvolá.

Záměr zpracovává zástupce odboru, jehož činnost má uvažovaný systém podporovat především, spolu se zástupcem odboru informačních technologií.

Před postupem do dalšího zpracování musí být záměr **schválen** příslušným odborem a vedením krajského úřadu či radou kraje.

##### 6.1.2.2 Výběr

Výběr nového IS znamená v první řadě podrobnou definici funkčních, kvalitativních, bezpečnostních a časových požadavků, SLA parametrů, mechanismů následné správy, požadavků na dokumentaci, požadavků na projektové řízení dodavatele, implementaci, testovací provoz, akceptaci, školení apod. U projektů delších než 1 rok nebo u projektů, kde finanční náročnost dodávky přesáhne 2 miliony Kč, je vyžadováno projektové řízení na straně dodavatele dle ISO/ČSN 10006 Směrnice pro management jakosti projektu.

Výběr musí být prováděn v souladu s pravidly pro výběrová řízení.

Před postupem do dalšího zpracování musí být výběr **schválen** příslušným odborem a vedením krajského úřadu či radou kraje a provedeny další nezbytné kroky pro zajištění realizace.

### 6.1.2.3 Implementace

Dle rozsahu IS je po dodavateli před započítáním vlastních implementačních prací vyžadován **implementační projekt** nebo **implementační studie**. Tato dokumentace musí být **schválena** pověřeným zástupcem krajského úřadu a průběžně dodavatelem **aktualizována** tak, aby byla v souladu se skutečností. Před předáním IS do testovacího provozu je dodavatel povinen dodat **provozní dokumentaci**.

Implementace musí být provedena v definovaných etapách podle implementační dokumentace v souladu se závěry výběrového řízení. Jednotlivé etapy budou zodpovědní pracovníci přebírat postupně podle schváleného **harmonogramu**.

Implementaci řídí zástupce odboru informačních technologií s podporou zástupce odboru, který bude daný IS nejlépe využívat.

### 6.1.2.4 Testovací provoz

Na vlastní implementaci navazuje testovací provoz, jehož cílem je ověřit splnění všech funkčních, kvalitativních a bezpečnostních požadavků a odstranění případných závad. Testování je prováděno vždy tak, aby nenarušilo běžný provoz ani bezpečnost provozovaných IS a zpracovávaných dat. Testování se děje podle předem stanoveného plánu na vyčleněném HW a na cvičných datech, která neobsahují osobní nebo citlivé údaje (viz zákon č. 101/2000 Sb.).

Úspěšné absolvování všech testů a splnění všech požadavků včetně požadavků na dokumentaci je potvrzeno podpisem **akceptačního protokolu**.

Splnění funkčních požadavků ověřuje a potvrzuje zástupce odboru, jehož činnost má uvažovaný systém podporovat především, kvalitativní a bezpečnostní požadavky a požadavky na dokumentaci ověřuje a potvrzuje zástupce odboru informačních technologií.

### 6.1.2.5 Školení

Před spuštěním ostrého provozu musejí být dotčení uživatelé nového IS řádně proškoleni.

Školení organizuje zástupce odboru, jehož činnost má uvažovaný systém podporovat především.

### 6.1.2.6 Ostrý provoz

Ostrý provoz zahrnuje procesy běžné údržby, správy, kontrolu dodržování přijatých pravidel, řízení změn IS a případně řízený zánik IS. Tyto činnosti jsou dále podrobně popsány v následujících odstavcích.

## 6.2 Zásady a postupy pro provozování IS

Veškeré činnosti související se správou IS musejí být prováděny v souladu s touto informační koncepcí a s navazující provozní dokumentací IS.

Základní činnosti správy IS budou prováděny interními pracovníky krajského úřadu dle následujících zásad:

- každý IS musí mít určeného správce, bezpečnostního správce a klíčového uživatele – zaměstnance úřadu.
- každý IS v ostrém provozu musí být zařazen do jednotného monitoringu

- každý IS v ostrém provozu musí být zálohován a zejména musejí být zálohována data v něm zpracovávaná.
- veškeré prováděné činnosti musejí být zaznamenávány do provozní dokumentace.
- provozní dokumentace musí být udržována aktuální tak, aby vždy odrážela reálný stav IS.
- údržba IS může být prováděna jen takovým způsobem a v takových časových obdobích, aby nebyl narušen chod úřadu a ohrožena bezpečnost IS a zpracovávaných dat.
- pokud je potřeba provést odstávku IS v pracovní době úřadu, musí být čas a rozsah prací předem schválen vedoucím dotčeného odboru a navíc musejí být informováni všichni uživatelé dotčeného IS a to minimálně s 24 hodinovým předstihem.

Pro jednotlivé specifické činnosti (např. upgrade IS nebo jeho subsystému na novou verzi bez změny funkčnosti – např. databáze) mohou být využiti externí pracovníci (typicky zaměstnanci dodavatelských společností) za těchto podmínek:

- za řízení činností zodpovídá vždy pověřený pracovník krajského úřadu.
- přístup k IS je povolován vždy jen v nezbytném rozsahu a na omezenou (nezbytně nutnou) dobu.
- přístup je povolován vždy konkrétnímu pracovníkovi dodavatele (tj. ne paušálně celé dodavatelské firmě).
- pracovník dodavatele musí být seznámen s provozními a bezpečnostními předpisy IS a musí se písemně zavázat je dodržovat
- veškeré prováděné činnosti musejí být zaznamenávány do provozní dokumentace

Kontrolu dodržování výše uvedených zásad provádí vedoucí odboru informačních technologií. Navíc je 1x ročně prováděna útvarem interního auditu celková revize dodržování informační koncepce včetně kontroly dodržování všech výše uvedených zásad.

## 6.3 Řízení změn v IS

Změnou se rozumí taková úprava IS, která znamená

- změnu funkčnosti IS (tj. rozšíření nebo zúžení počtu, rozsahu nebo funkcionality služeb poskytovaných IS).
- změna konfigurace IS (změna HW, topologie, adresace, nastavení nebo dalších parametrů systému).
- změna uživatelského rozhraní.
- změna datového rozhraní.

Veškeré změny musejí být prováděny řízeným způsobem v níže uvedených krocích:

1. Záměr
3. Implementace
4. Testovací provoz
5. Školení

## 6. Ostrý provoz

Jednotlivé kroky jsou podrobněji popsány v odstavci 6.1.2, proto jsou i stejně číslovány.

### 6.4 Ukončení činnosti IS

Ukončení činnosti IS je zvláštním druhem změny. Opět je potřeba tuto změnu provést řízeným způsobem a to v následujících krocích:

1. Záměr
2. Implementace - zpřístupnění
3. Testovací provoz bez systému
4. Ostrý provoz - odinstalace

#### 6.4.1.1 Záměr

V úvodní fázi je definována potřeba nového ukončení provozu IS, stanoveny funkční, kvalitativní a bezpečnostní požadavky, je uvedena analýza výchozího stavu a popsán stav cílový. Je též odhadnuta finanční, personální a časová náročnost a analyzovány dopady, které ukončení provozu IS vyvolá.

Záměr zpracovává zástupce odboru, jehož činnost uvažovaný systém podporoval především, spolu se zástupcem odboru informačních technologií.

Před postupem do dalšího zpracování musí být záměr **schválen** příslušným odborem a vedením krajského úřadu či radou kraje.

#### 6.4.1.2 Implementace - zpřístupnění

Dle rozsahu IS je před započítáním vlastních implementačních prací vyžadován **implementační projekt** nebo **implementační studie**. Tato dokumentace musí být **schválena** pověřeným zástupcem krajského úřadu a průběžně **aktualizována** tak, aby byla v souladu se skutečností. Před odinstalací IS aktualizovat **provozní dokumentaci**.

Implementace musí být provedena v definovaných etapách podle implementační dokumentace v souladu se závěry výběrového řízení. Jednotlivé etapy budou zodpovědní pracovníci přebírat postupně podle schváleného **harmonogramu**.

Implementaci řídí zástupce odboru informačních technologií s podporou zástupce odboru, který bude daný IS nejvíce využívat.

#### 6.4.1.3 Testovací provoz

Na vlastní implementaci navazuje testovací provoz, jehož cílem je ověřit splnění všech funkčních, kvalitativních a bezpečnostních požadavků a odstranění případných závad od zpřístupnění IS. Testování je prováděno vždy tak, aby nenarušilo běžný provoz ani bezpečnost provozovaných IS a zpracovávaných dat. Testování se děje podle předem stanoveného plánu na vyčleněném HW a na cvičných datech, která neobsahují osobní nebo citlivé údaje (viz zákon č. 101/2000 Sb.).

Úspěšné absolvování všech testů a splnění všech požadavků včetně požadavků na dokumentaci je potvrzeno podpisem **akceptačního protokolu**.



Splnění funkčních požadavků ověřuje a potvrzuje zástupce odboru, jehož činnost má uvažovaný systém podporovat především, kvalitativní a bezpečnostní požadavky a požadavky na dokumentaci ověřuje a potvrzuje zástupce odboru informačních technologií.

#### **6.4.1.4 Ostrý provoz**

Ostrý provoz zahrnuje řízený zánik IS. Tyto činnosti jsou dále podrobně popsány v následujících odstavcích.

V Záměru musí být navíc uvedeno:

- jaké jsou důvody pro ukončení IS,
- jak bude naloženo s daty – zda budou data převedena do nových IS, zda budou archivována nebo skartována,
- jak bude naloženo s technickým zařízením odstavovaného IS – zda bude ponecháno v majetku a správě krajského úřadu, zda bude prodáno, darováno, ekologicky zlikvidováno apod.

## **7 Financování IS**

Financování rozvoje IS i jeho správy a údržby bude prováděno v souladu s rozpočtovými pravidly kraje z jeho rozpočtu.

**Plán financování** záměrů na pořízení, příp. vytvoření IS, financování správy a údržby IS a financování dlouhodobých cílů v oblasti kvality i bezpečnosti IS zpracovává pověřený pracovník odboru informačních technologií a ke schválení vedení kraje předkládá vedoucí odboru informačních technologií jako součást Plánu rozvoje IS, který je součástí rozpočtu daného roku. Aktualizace plánu, jeho kontrola a schvalování se provádí v **roční** periodicitě.

## 8 Naplňování informační koncepce a řízení změn

### 8.1 Dodržování informační koncepce

Naplňování informační koncepce znamená

- uplatňování zásad uvedených v informační koncepci při běžném provozu a údržbě IS,
- udržování informační koncepce v aktuálním stavu a v souladu se skutečností,
- pravidelné vyhodnocování dodržování informační koncepce,
- realizaci opatření pro odstranění zjištěných nedostatků.

Za jednotlivé oblasti a činnosti popsané v informační koncepci musí být stanovena osobní zodpovědnost konkrétních zaměstnanců úřadu. Tato otázka je dále popsána v kapitole 9.

### 8.2 Kontrola dodržování informační koncepce

Vyhodnocování dodržování informační koncepce je základním kontrolním mechanismem zajišťujícím zpětnou vazbu. Základním principem je oddělení výkonné a kontrolní role – tj. **vyhodnocování musí provádět jiný pracovník, než ten, který je zodpovědný za naplňování informační koncepce.** Totéž platí pro vyhodnocování dílčích oblastí, pro které byla stanovena konkrétní dílčí odpovědnost.

Vyhodnocování dodržování informační koncepce se děje **1x ročně** a to synchronně s aktualizací informační koncepce.

Vyhodnocování řídí pracovník stanovený v kapitole 9. Pro vyhodnocování dílčích oblastí může přizvat odborníky na tyto oblasti, avšak musí přitom dodržet výše uvedenou nezávislost vyhodnocující osoby na osobě odpovědné za realizaci informační koncepce v dané oblasti.

Všechny činnosti, jejichž provádění je posuzováno, jsou porovnávány s informační koncepcí platnou v době, kdy byla daná činnost prováděna – na to je nutné dbát v případě, že došlo za uplynulých 12 měsíců ke změně informační koncepce.

#### 8.2.1 Oblasti pro kontrolu dodržování informační koncepce

Kontrola dodržování informační koncepce bude probíhat v následujících oblastech:

##### Oblast charakteristik IS:

- informační koncepce obsahuje popis všech IS,
- informační koncepce obsahuje všechny vazby provozních IS na IS,
- popis IS a případných vazeb je včas aktualizován,
- předpokládané změny IS jsou průběžně zaznamenávány.

##### Oblast záměrů pořízení nebo vytvoření nových IS:

- informační koncepce obsahuje všechny záměry na pořízení nových IS,
- jednotlivé záměry jsou zpracovány dle požadavků informační koncepce,
- všechny projekty v této oblasti byly realizovány dle postupů definovaných v informační koncepci.
- všechna výběrová řízení probíhají v souladu s předpisy jak interními, tak externími.

**Oblast řízení kvality:**

- 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.

**Oblast řízení bezpečnosti:**

- 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.

**Oblast správy IS:**

- jsou uplatňovány zásady a postupy pro plánování rozvoje IS.
- jsou uplatňovány zásady a postupy pro zajištění provozu a údržby IS – posuzuje se též vhodnost a účinnost kontrolních mechanismů,
- jsou uplatňovány zásady a postupy pro řízení změn IS,
- jsou uplatňovány zásady a postupy pro ukončení činnosti IS.

**Oblast financování IS:**

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

**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.

**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.

## **8.2.2 Zápis z kontroly dodržování informační koncepce**

Pracovník odpovědný za provádění vyhodnocování dodržování informační koncepce zodpovídá též za vyhotovení zápisu. Zápis musí být vytvořen z každého vyhodnocování a musí obsahovat:

- identifikační údaje (označení verze informační koncepce, které se týká, datum vyhotovení, jména zpracovávajících a zodpovědné osoby, atd.),
- popis provedených vyhodnocení a jejich výsledky a závěry,
- popis navržených opatření k nápravě případně zjištěných nedostatků včetně stanovení zodpovědností a termínů,
- záznam o schválení zápisu.

### 8.3 Řízení změn informační koncepce

Informační koncepce musí být udržována aktuální a v souladu se skutečným stavem, v souladu s požadavky Olomouckého kraje a s platnou legislativou. Proto je prováděna její pravidelná **revize** a to **1x ročně** synchronně s vyhodnocováním dodržování informační koncepce.

Změny navrhuje pověřený zástupce odboru informačních technologií a ke schválení vedení kraje předkládá vedoucí odboru informačních technologií a to minimálně **s měsíčním předstihem** před datem navrhovaného počátku platnosti nové verze informační koncepce.

Změny informační koncepce budou vždy prováděny formou vydání **nové verze** informační koncepce. **Číslo** verze informační koncepce se skládá z čísla verze a podverze, přičemž číslo **verze** bude změněno vždy při zásadnější změně (např. uvedení nového IS do provozu, vyřazení stávajícího IS z provozu, výrazné změny v organizační struktuře, v legislativě, ve funkcích IS a jejich poskytování uživatelům, v dlouhodobých cílech apod.). Číslo **podverze** bude změněno při drobnější úpravě informační koncepce.

Bude vždy uveden popis změny, kdo změnu do informační koncepce zapracoval, kdo nové znění schválil, kdy a datum, od kterého je nová verze informační koncepce platná.

Dále bude uveden odkaz na dokument obsahující novou verzi informační koncepce, počet stran, počet příloh a statut (v průběhu zpracovávání „draft“, dále např. „k oponentuře“, „ke schválení“, „schváleno“, „neplatné“).

S novou schválenou verzí informační koncepce musí být prokazatelně seznámeni všichni pracovníci, jichž se informační koncepce nějak dotýká.

## 9 Organizace řízení a odpovědnosti

### 9.1 Základní principy řízení kvality a bezpečnosti IS

Systém řízení kvality a bezpečnosti IS není dokončený stav, ale proces, který podléhá neustálé kontrole a zlepšování. Tyto změny se dějí v cyklu (v tzv. PDCA cyklu), který se skládá z následujících aktivit:

1. **Plánování.** Přípravná fáze, plánování opatření, plánování implementace, vytvoření Plánu rozvoje IS, definice dlouhodobých cílů v oblasti kvality a bezpečnosti IS apod.
2. **Implementace.** Provedení plánovaných akcí z předchozí fáze, zavedení opatření, nastavení kontrolních mechanismů apod.
3. **Kontrola.** Nezávislý audit a kontrola fází plánování i implementace, vyhodnocení, zda splňuje zadání a předepsané postupy, zda přináší kýžený efekt apod.
4. **Revize.** Návrh na zlepšení na základě výsledků fáze kontroly, návrh opatření ke zlepšení, návrh změn procesů, konfigurace, Informační koncepce, plánů, provozní dokumentace atd.

Ve všech těchto fázích je možné povolát na pomoc externí konzultační společnost.

### 9.2 Výkon řízení kvality a bezpečnosti IS

Řídící infrastruktura je definována v souladu s organizačním řádem úřadu. Stanovuje funkce a jejich zodpovědnosti za jednotlivé činnosti v oblasti dlouhodobého řízení IS. Jsou stanoveny zvlášť pro

- řízení realizace informační koncepce a
- řízení činností ke splnění zákonných povinností.

#### 9.2.1 Řízení realizace informační koncepce

Za činnosti vedoucí k dosažení cílů, naplňování zásad a uplatňování definovaných postupů celkově zodpovídá **odbor informačních technologií**.

Tabulka č. 17: Realizace informační koncepce

Oblast	Zpracovává	Schvaluje
Plán rozvoje IS	vedoucí odboru informačních technologií	ředitel krajského úřadu
Plán financování IS	vedoucí odboru informačních technologií	rada Olomouckého kraje
Řízení kvality IS (stanovování dlouhodobých cílů kvality a konkrétních požadavků na kvalitu IS, sestavení a údržba plánu řízení kvality, vyhodnocování naplnění požadavků a dodržování plánu)	vedoucí odboru informačních technologií	ředitel krajského úřadu
Řízení bezpečnosti IS (stanovování dlouhodobých cílů bezpečnosti a konkrétních požadavků na bezpečnost IS, sestavení a údržba plánu řízení bezpečnosti, vyhodnocování naplnění požadavků a dodržování plánu)	vedoucí odboru informačních technologií	ředitel krajského úřadu
Pořizování a vytváření IS (včetně zajištění veřejných soutěží apod.)	vedoucí odboru informačních technologií	ředitel krajského úřadu
Zajištění provozu a údržby IS	vedoucí odboru informačních technologií	ředitel krajského úřadu
Řízení změn IS	vedoucí odboru informačních technologií spolu s vedoucím toho odboru, který zodpovídá za dotčenou agendu	ředitel krajského úřadu
Řízení ukončování provozu IS	vedoucí odboru informačních technologií s vedoucím toho odboru, který zodpovídá za dotčenou agendu	ředitel krajského úřadu
Vyhodnocování dodržování souladu provozování IS	vedoucí odboru informačních technologií	ředitel krajského úřadu
Aktualizace informační koncepce	vedoucí odboru informačních technologií	ředitel krajského úřadu
Vyhodnocování dodržování informační koncepce a vyhotovení zápisu o něm	vedoucí odboru informačních technologií	ředitel krajského úřadu
Opatření k nápravě	vedoucí odboru informačních technologií	ředitel krajského úřadu

### 9.2.2 Řízení činností ke splnění zákonných povinností

Podrobněji jsou dílčí odpovědnosti uvedeny v následující tabulce.

Tabulka č. 18: Řízení činností ke splnění zákonných povinností

Zákon	Popis	Realizuje
zák. č. 365/2000 Sb. §5 odst. 2 písm. a	spolupracovat s Ministerstvem vnitra při plnění jeho úkolů podle § 4 odst. 1	ředitel krajského úřadu

<b>Zákon</b>	<b>Popis</b>	<b>Realizuje</b>
zák. č. 365/2000 Sb. §5 odst. 2 písm. a	spolupracovat s Ministerstvem vnitra při provádění kontroly na místě dle zákona o státní kontrole	ředitel krajského úřadu
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, pokud tato povinnost vyplývá ze zákona č. 218/2000 Sb.	vedoucí odboru informačních 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, pokud tato povinnost vyplývá ze zákona č. 218/2000 Sb.	vedoucí odboru informačních technologií
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	vedoucí odboru informačních technologií
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, pokud je správcem příslušných datových prvků.	vedoucí odboru informačních technologií
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	vedoucí odboru informačních technologií
zák. č. 365/2000 Sb. §5 odst. 2 písm. d	prokázat atestem způsobilost informačního systému k realizaci výše uvedených vazeb	vedoucí odboru informačních technologií
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 IS a IS o DP	vedoucí odboru informačních technologií
zák. č. 365/2000 Sb. §5 odst. 2 písm. f	Uveřejňovat informace související s výkonem veřejné správy způsobem, který umožňuje dálkový přístup a ve formě přístupné i pro osoby se zdravotním postižením (dle Vyhlášky č. 64/2008 Sb.).	vedoucí odboru informačních technologií
zák. č. 365/2000 Sb. §5 odst. 2 písm. g	odstranit zjištěné nedostatky ve lhůtě stanovené Ministerstvem vnitra	vedoucí odboru informačních technologií
zák. č. 365/2000 Sb. §5a odst. 1	vytvářet a vydávat informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování	vedoucí odboru informačních technologií

Zákon	Popis	Realizuje
zák. č. 365/2000 Sb. §5a odst. 2	vytvářet a vydávat provozní dokumentaci k jednotlivým IS, uplatňovat ji v praxi a vyhodnocovat její dodržování	vedoucí odboru informačních technologií
zák. č. 365/2000 Sb. §5a odst. 3	zajistit si atest dlouhodobého řízení IS	vedoucí odboru informačních technologií
zák. č. 365/2000 Sb. §5b odst. 1 až odst. 2	zajišťovat bezpečnost IS v rozsahu odpovídajícím alespoň minimálním bezpečnostním požadavkům k zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací dle prováděcího předpisu	vedoucí odboru informačních technologií



## 10 Seznam příloh

1. Příloha č. 1: ISVS ve správě Olomouckého kraje a vazby na další IS
2. Příloha č. 2: Katalog informačních systémů ve správě Olomouckého kraje
3. Příloha č. 3: Plán rozvoje informačních systémů
4. Příloha č. 4: Plán financování informačních systémů