INFORMAČNÍ KONCEPCE ISVS

SZPI BRNO

Tabulka 1 - Náležitosti označení IK

Informační koncepce 4.0			
Název organizace:	Státní zemědělská a potravinářská inspekce		
IČ:	75014149		
Adresa:	Květná 15, 603 00 Brno		
Datum změny:	Autor:	Funkce:	Útvar:
27. 5. 2025	Ing. Pavel Frybert	Manažer kybernetické bezpečnosti	OI OKÚ
Datum schválení:	Schválil:	Funkce:	Útvar:
-	Mgr. Jaroslav Stross	Ředitel odboru kancelář úřadu (OKÚ)	OKÚ
Datum platnosti od:	Označení verze	Název souboru:	
27. 5. 2021	4.0	Informační koncepce v4.docx	
Datum platnosti do:	Počet stran:	Umístění souboru:	
26. 5. 2026	15	Intranetový portál Web SZPI	
Doba platnosti:	Počet příloh:		
5 let	1		

Tabulka 2 - Historie změn

Datum změny:	Popis změny:	Důvod změny:	Identifikace změny:
29. 4. 2022	Vyhodnocení	Roční vyhodnocení	Revize požadavků na jakost a bezpečnost 2022.
28. 4. 2023	Vyhodnocení	Roční vyhodnocení	Revize požadavků na jakost a bezpečnost 2023.
31. 4. 2024	Vyhodnocení	Roční vyhodnocení	Revize požadavků na jakost a bezpečnost 2024.
27. 5. 2025	Nový dokument, vyhodnocení	Končící doba platnosti IK v3 ke dni 27. 5. 2025, změny dle vyhlášky č. 360/2023 Sb.	Nová verze dokumentu (IK v4.0), rozšíření Zdrojových tabulek, revize požadavků na jakost a bezpečnost.

Obsah:

Úvod

Dokument Informační koncepce ISVS (dále také *IK*) tvoří základ pro řešení dlouhodobého řízení informačních systémů veřejné správy Státní zemědělské a potravinářské inspekce Brno (dále také *SZPI*) v souladu s požadavky zákona č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen *Zákon*) a vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy (dále jen *Vyhláška*).

Účelem dokumentu IK je:

- identifikovat a dokumentovat stávající a nově budované informační systémy veřejné správy (dále jen *ISVS*), případně provozní informační systémy (dále jen *PIS*) s vazbami na ISVS, jejich stav, aktuálnost, potenciál a záměry do budoucna,
- definovat dlouhodobé cíle a konkrétní požadavky týkající se ISVS v souladu s IKČR.
- popsat zásady a postupy řízení ISVS.

IK SZPI včetně změn a doplňků projednává a schvaluje *Ředitel OKÚ SZPI*.

IK je závazná pro všechny zainteresované útvary SZPI, zaměstnance v řídících a výkonných funkcích a všechny zaměstnance SZPI a ostatní pracovníky ve smluvním vztahu k SZPI v rámci jejich pracovní náplně či stanoveného rozsahu vykonávaných činností souvisejících s ISVS SZPI.

Struktura bezpečnostních rolí je stanovena a dokumentována s ohledem na požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen ZoKB) a vyhlášky č. 317/2014 Sb., o významných informačních systémech.

1. IDENTIFIKACE INFORMAČNÍ KONCEPCE ISVS

Informační koncepce ISVS je dokument, který není v čase neměnný, je zpracován vždy s platností na určité období a podléhá potřebám změn:

- ať už se jedná o změny náhlé, vynucené změněnou situací či okolnostmi, novými skutečnostmi,
- nebo se jedná o pravidelné revize s cílem ověřit shodu, případně odhalit nesoulad s aktuálním stavem a zejména budoucím rozvojem, strategickými cíli, plány a záměry v oblasti dlouhodobého řízení ISVS.

Ze všech těchto důvodů je důležité jednoznačné rozlišení nových verzí a zachování historie dokumentu. Tento požadavek zajišťuje pevně dané označení informační koncepce s veškerými náležitostmi v úvodu dokumentu, viz úvodní kapitola, Tabulka 1 - Náležitosti označení IK a Tabulka 2 - Historie změn, kde jsou chronologicky od nejnovější po nejstarší řazeny všechny verze dokumentu a jejich změny. Každá další verze dokumentu musí splňovat stanovené náležitosti označení.

Slovník použitých zkratek a pojmů

Zkratka:	Význam:
ČR	Česká republika
ČSN EN	Česká státní norma (z pův. Československá státní norma), Evropská norma
ICI	Information and Communication Infrastructure (Informační a komunikační infrastruktura)
IK	Informační koncepce
IS	Informační systém
ISDS	Informační systém datových schránek
ISMS	Information Security Management System (systém řízení bezpečnosti informací)
ISO IEC	Mezinárodní organizace pro normalizaci, Mezinárodní elektrotechnická komise (International Organization for Standardization, International Electrotechnical Commission)
ISVS	Informační systém veřejné správy
IT / ICT	Informační technologie/informační a komunikační technologie
OI	Oddělení informatiky
OKÚ	Odbor kancelář úřadu
OVS / OVM	Orgán veřejné správy/orgán veřejné moci
PD	Provozní dokumentace
PIS	Provozní informační systém
SZPI	Státní zemědělská a potravinářská inspekce
TPP	Technické a programové prostředky
AIS	agendový informační systém (KOPR, GINIS)
ZoKB	Zákon o kybernetické bezpečnosti (zák. č. 181/2014 Sb.)
VP	Vedoucí pozice
OP	Operativní porada
PnP	Potraviny na pranýři

2. Informační systémy ve správě SZPI

Aktuální seznam všech ISVS, případně PIS s vazbami na ISVS obsahuje samostatná příloha v souboru Zdrojové tabulky IK v4.xlsx, list Přehled a popis ISVS vždy v poslední aktuální verzi.

1. ISVS:
    - Informační systém Kontrolní, laboratorní a právní činnost (dále jen IS KOPR)
        - který je významným informačním systémem dle ZoKB
        - s vazbou na ERMS, Víno, GINIS
    - Informační systém Víno (dále jen Víno)
        - který je významným informačním systémem dle ZoKB
    - Spisová služba ERMS (dále jen ERMS)
        - který je významným informačním systémem dle ZoKB
        - s vazbou na KOPR, Víno, Exchange a DS SZPI
    - Webový portál (dále jen Web)
        - s vazbou na portál Potraviny na pranýři (PnP)
    - Internetový portál Potraviny na pranýři (PnP)
        - s vazbou na KOPR
    - GINIS
        - s vazbou na ERMS, KOPR, IISSP
    - Exchange
        - který je významným informačním systémem dle ZoKB
        - s vazbou na ERMS
2. PIS:
    - Modul Datové schránky SZPI (dále jen DS SZPI)
        - s vazbou na ISDS (jiného správce)
    - Docházkový systém
        - s vazbou na GINIS, Exchange
    - Intranetový portál (Podnikový intranet)
    - Videokonferenční systém
        - s vazbou na Exchange

2.1. Popis ISVS

Pro účely informační koncepce byla zvolena následující metoda popisu:

- Jednotlivé ISVS jsou v této příloze popisovány každý zvlášť;
- Jsou popisovány pouze vazby PIS na ISVS, ostatní PIS nejsou popisovány.

V zájmu zachování jednotné evidence ISVS a prevence duplicity:

- jsou pro účely IK dále uvedeny pouze odkazy na popis identifikovaných ISVS jako podsystémů IS SZPI zahrnujících jednotlivé moduly, dostupné na Webovém portálu SZPI:

  Hlavní stránka - Činnost SZPI - Informační systém - Informační systém SZPI

- je aktuální zdroj těchto dat zpracován v příloze - v samostatném souboru *Zdrojové tabulky IK v4.xlsx*, na listu *„Přehled a popis ISVS“*. V tomto souboru jsou uvedeny veškeré Vyhláškou požadované náležitosti každého ISVS, které se týkají jeho popisu, správců a uživatelů, vazeb s jinými systémy, související legislativy, dokumentace systému, aktuálního stavu a uvažovaných změn, přičemž některé detaily jsou řešeny formou odkazů, tzn. že:
    - provozní dokumentace k systémům je dostupná v jednotném úložišti na intranetovém portálu v samostatné sekci, u vybraných systémů pak přímo v nich.
    - detailní popisy ISVS v oblasti používaných technických a programových prostředků jsou řešeny v příslušných vnitřních předpisech, které jsou řešeny samostatně pro každý ze systémů, technické popisy jsou sdíleny prostřednictvím odkazu na technickou dokumentaci k IT-infrastruktuře SZPI na

Intranetu a pro vybrané systémy jsou k dispozici zdrojové kódy, dostupné v kanceláři Ř OKÚ v zajištěném trezoru.

2.2. Související právní předpisy

Právní předpisy, jimiž se SZPI řídí při výkonu své činnosti, jsou dostupné na webovém portálu SZPI – v části „Informace nejen pro začínající podnikatele“.

Jednotlivé zákonné předpisy, na jejichž základě jsou provozovány a spravovány identifikované informační systémy veřejné správy, jsou uvedeny níže v kapitole č. 10 – Související dokumentace.

Související legislativa pro každý ISVS, případně i PIS, pokud má vazby na jiné ISVS, je uvedena v souboru *Zdrojové tabulky IK v4.xlsx* na listu *„Přehled a popis ISVS“*.

3. ZÁMĚRY NA POŘÍZENÍ NEBO VYTVOŘENÍ NOVÝCH ISVS

Záměry na pořízení nového ISVS jsou popisovány a předkládány operativní poradě, v případě schválení jsou dále rozvedeny v rámci zadávací dokumentace VZ. Detaily jsou dále v rámci dlouhodobého řízení ISVS uváděny v samostatné příloze, viz soubor *Zdrojové tabulky IK v4.xlsx na listu „Záměry“*.

4. ŘÍZENÍ BEZPEČNOSTI ISVS

Definice cílů i požadavků na ISVS vždy zohledňují vyhlášku o dlouhodobém řízení ISVS a IKČR.

Cíle a požadavky na ISVS jsou popsány v samostatné příloze v souboru *Zdrojové tabulky IK v4.xlsx* na listu III. Cíle a požadavky.

Jakost ISVS je zahrnuta do rámce řízení jakosti podle požadavků systému managementu jakosti – ČSN EN ISO 9001:2016 – podpořeného certifikátem, jehož je organizace držitelem.

Bezpečnost ISVS je zahrnuta do řízení bezpečnosti podle požadavků ZoKB.

Výstup z obou systémů řízení umožňuje definovat plány, jak má být cílů, resp. požadavků na bezpečnost ISVS dosaženo.

4.1. Cíle, požadavky a plány řízení a implementace ISVS

Zavedení a neustálé zlepšování ISVS je řízeno prostřednictvím definovaných cílů a požadavků, viz soubor *Zdrojové tabulky IK v4.xlsx* na listu *„Cíle a požadavky“*.

Vize a cíle *Koncepce rozvoje informační a komunikační infrastruktury SZPI* jsou založeny na strategických dokumentech SZPI (viz např. Politika kybernetické bezpečnosti) kladou důraz na důvěryhodnost a bezpečnost prostředků zpracování dat nejen ve vztahu k veřejnosti, ale vychází z nich také definice dlouhodobých bezpečnostních cílů a požadavků na ISVS a kybernetickou bezpečnost obecně.

Komplexní a systematické řízení informační bezpečnosti jako celku zahrnujícího všechny informační systémy, zajišťuje implementace systému řízení bezpečnosti informací v souladu s požadavky ZoKB, se kterými korespondují definované bezpečnostní cíle a požadavky kladené na ISVS.

5. ZÁSADY A POSTUPY PRO SPRÁVU ISVS

SZPI řídí provozování ISVS prostřednictvím stanovených postupů, které rozlišují následující činnosti:

- pořizování (příp. vytváření) nových ISVS,
- provozování stávajících ISVS, zahrnující:
    - provoz a údržbu,

- změny a rozvoj,
- ukončení činnosti.

Všechny postupy správy ISVS vyžadují vždy stanovení složky výkonné a kontrolní. Každá z uvedených skupin činností má proto určeny odpovědné funkce / osoby pro podávání návrhů, pro jejich schvalování a pro realizaci schválených návrhů, definované v rámci pracovních skupin, a jsou určeni garanti, kteří odpovídají za dané ISVS.

5.1. Pořizování a vytváření ISVS

SZPI řeší potřeby nových ISVS výhradně formou pořízení od externího dodavatele, vlastními silami nové IS/ISVS nevytváří. Proces pořizování/nákupu ISVS je řízen prostřednictvím Operativní porady.

Postupy při pořizování ISVS jsou zahrnuty do standardního projektového řízení a obsahují požadavky dle vyhlášky o ISVS, viz soubor *Zdrojové tabulky IK v4.xlsx* na listu *„Řížení živ. cyklu “*.:

Pro realizaci činností, které je nutno zpracovat při pořizování ISVS, slouží standardní interní postupy popsané v interních předpisech SZPI.

6. ZPŮSOB FINANCOVÁNÍ ISVS

Způsob financování ISVS je dán interním předpisem OS 003/2006 *Zásady rozpočetnictví*, který stanovuje zásady tvorby rozpočtu SZPI, včetně zásad tvorby a použití peněžních fondů (viz kapitola č. 10 – Související dokumentace).

Postupy při financování ISVS (informačních systémů veřejné správy):

Financování informačních systémů je v souladu s pravidly danými obecnými předpisy v této oblasti:

- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (ve znění pozdějších předpisů),
- zákon č. 134/2016 Sb., o zadávání veřejných zakázek (ve znění pozdějších předpisů),
- zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (ve znění pozdějších předpisů),
- zákon č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích (ve znění pozdějších předpisů),
- vyhláška č. 560/2006 Sb. o účasti státního rozpočtu na financování programů reprodukce majetku (v platném znění)

Financování informačních systémů akceptuje:

- Usnesení vlády České republiky ze dne 27. 1. 2020 č. 86 o uložení povinností informovat Digitální a informační agenturu v souvislosti s výdaji v oblasti informačních a komunikačních technologií, a přílohu:
- Základní zásady postupu při posuzování záměrů výdajů v oblasti informačních a komunikačních technologií.

Financování je řešeno vlastním rozpočtem SZPI vydaným ze Státní pokladny.

Jsou definovány následující povinnosti:

- v oblasti schvalování investičních záměrů Ministerstvem zemědělství;
- při zadávání veřejných zakázek na ISVS a zakázek malého rozsahu na ISVS, např.:
  - požadavky na testování IS před jejich akceptací,
  - požadavky na akceptační protokoly,
  - požadavky na technickou podporu, příp. školení uživatelů ISVS,

- požadavky na certifikaci jakosti IS, případně řízení jakosti a bezpečnosti u dodavatele apod.

Za proces zadávání zakázek v oblasti ISVS a při činnostech v oblasti získávání finančních prostředků na realizaci záměrů v této oblasti nese zodpovědnost příslušná funkce/role určená v souladu s platnými interními předpisy.

Financování ISVS se řeší pro všechny tři oblasti obdobně:

- financování záměrů na pořízení nebo vytvoření nových ISVS,
- financování naplnění dlouhodobých cílů ISVS, včetně způsobu zajištění potřebných zdrojů,
- financování správy ISVS zahrnující provoz, údržbu a rozvoj ISVS, a další podpůrné činnosti.

Způsob financování uvedených oblastí (záměrů, projektů a správy ISVS) je upraven v interních předpisech týkajících se zákona č. 134/2016 Sb., o zadávání veřejných zakázek, viz organizační směrnice:

- č. 002/2003 – Postup při zadávání veřejných zakázek
- č. 009/2003 – Vnitřní kontrolní systém SZPI
- č. 021/2003 – Hospodaření SZPI s majetkem České republiky
- č. 002/2014 – Uzavírání a evidence smluv
- a další interní předpisy zveřejněné na intranetu SZPI

7. NAPLŇOVÁNÍ INFORMAČNÍ KONCEPCE

7.1. Postupy při provádění změn IK

Změny v IK formou vydání nové verze IK provádí osoba ve funkci *manažer kybernetické bezpečnosti* SZPI, a to na základě definovaného postupu změnového řízení, viz interní předpis *Pravidla pro tvorbu, aktualizaci, evidenci a distribuci vnitřních předpisů OS 001_03_text.*

Postup při provádění změn IK:

- změny IK mohou být iniciovány prostřednictvím:
  - vzniku nového požadavku na pořízení/vytvoření/změnu/ukončení činnosti IS/ISVS,
  - průběžných změn nebo dokončení procesu implementace cílů a požadavků IS/ISVS,
  - závěrů z výsledků vyhodnocení plnění plánů řízení jakosti a bezpečnosti,
  - závěrů z revize IK,
  - zjištěné neshody IK s realitou,
  - změn v zákonných předpisech, normách, informační strategii, interních předpisech nebo z rozhodnutí nadřízených orgánů,
  - uplynutím data platnosti IK.
- Manažer kybernetické bezpečnosti:
  - zpracovává požadavek či návrh na změnu IK v rámci standardního změnového řízení,
  - stručně popíše změnu a důvod změny do historie změn v dokumentu IK,
  - jedná-li se o závažnou (podstatnou) změnu IK, předloží návrh dodatku či nového dokumentu IK ke schválení,
  - v případě navrhované dílčí změny zajistí její zapracování do dokumentu IK,
  - zajistí distribuci a zveřejnění nové verze IK.

Revize vlastního dokumentu IK a zdrojových tabulek k IK jsou prováděny v závislosti na počtu ISVS a vedených agend garantem dokumentu minimálně **1x za 1 rok**, příp. i dříve, pokud:

- došlo k organizační změně dotýkající se definovaných funkcí a odpovědností,

- vznikl nový záměr na pořízení ISVS,
- byla dokončena realizace nového ISVS,
- došlo k významným změnám v legislativě ovlivňující ISVS,
- vznikly nové požadavky v oblasti jakosti nebo bezpečnosti týkající se ISVS.

V případě zjištění potřeby promítnout významné změny do IK bude vydána její nová verze, nebo připojen dodatek.

7.1.1. Postup přípravy nové IK

S ohledem na potřebu zajistit, že před uplynutím doby platnosti dokumentu IK již bude vznikat nová IK, je stanoven termín pro zahájení přípravy nové IK nejpozději 2 měsíce před jejím vypršením, např. v rámci plánované pravidelné revize či aktualizace.

Za přípravu nové IK zodpovídá Manažer kybernetické bezpečnosti. Postup pro přípravu nové IK je shodný s postupem revize IK.

7.2. Postupy při vyhodnocování dodržování informační koncepce

Dodržování Informační koncepce musí být vyhodnocováno pravidelně minimálně **1x za 1 rok**.

Vyhodnocování by měla provádět osoba ve funkci, která nezodpovídá za realizaci IK, tj. obvykle představitel vedení pro jakost a manažer kybernetické bezpečnosti. Pro zápis o vyhodnocení slouží jednotný vzor s příslušnými kontrolovanými oblastmi v samostatné příloze v souboru *Zdrojové tabulky IK v4.xlsx* na listu *Šablona_Vyhodnocení IK*.

8. ODPOVĚDNOST ZA ŘÍZENÍ PROVÁDĚNÍ ČINNOSTÍ

8.1. Odpovědnosti za realizaci informační koncepce

Za oblast řízení provádění činností vedoucích k dosažení cílů, naplňování zásad a uplatňování postupů uvedených v této IK je zodpovědný vedoucí OI OKÚ.

Garantem dokumentu IK je osoba ve funkci Manažer kybernetické bezpečnosti IS SZPI.

Viz také *Zdrojové tabulky IK v4.xlsx* na listu *Řízení živ. cyklu (§14-21).*

9. PLÁN ŘÍZENÍ INFORMATIKY

9.1. Oblasti řízení informatiky

9.1.1. Strategie, plánování a organizace informatiky

Strategií, plánováním a organizací informatiky je v prostředí SZPI pověřeno oddělení informatiky Odboru kanceláře úřadu (dále OI OKÚ). Potřeby a soulad s celkovou digitální strategií ČR se stanovují interně na základě obecných porad OI, z nichž jsou konkrétní požadavky připravené k realizaci směrovány na porady Odboru kanceláře úřadu (dále OKÚ). Po schválení ředitelem OKÚ je požadavek na změnu/rozvoj dále řešen v rámci Operativní porady (dále OP). Veškeré požadavky jsou dohledatelné v rámci zápisů z předmětných porad. Hierarchie schvalovacích procesů, včetně následných kroků týkajících se veřejných zakázek, zacházení s veřejnými financemi apod. se řídí příslušnými vnitřními předpisy v rámci SMJ.

9.1.2. Pořizování a změny informačních systémů

Požadavky na pořízení/změnu informačních systémů mohou být zadávány jednotlivými zaměstnanci, odděleními, odbory, a to v souladu s příslušnými VP hierarchického řízení, kdy se na základě pokynu z OP konzultují konkrétně s OI. Podrobný postup je uveden ve směrnici OS_002_03.

9.1.3. Provozování informačních systémů

Za technický provoz informačních systémů v SZPI je odpovědné OI OKÚ, které zajišťuje přímou spolupráci s dodavateli a zajišťuje podkladový HW [redacted] OI OKÚ zajišťuje primární provoz technických prostředků HW – pravidelné aktualizace ve

spolupráci s dodavateli a nepřetržitý provoz, včetně zajištění pohotovostních služeb mimo pracovní dobu.

Funkční požadavky na informační systémy jsou zadávány funkčními garanty jednotlivých systémů a to vždy ve spolupráci s OI OKÚ. OI OKÚ zajišťuje kybernetickou bezpečnost daného systému v rámci svých kompetencí. Za kybernetickou bezpečnost jsou v prostředí SZPI zodpovědní i všichni zaměstnanci pracující v jednotlivých informačních systémech a to dle svých kompetencí a na základě pravidelného školení v oblasti kybernetické bezpečnosti.

Zaměstnanci OI OKÚ jsou určenými technickými garanty (technickými správci) daných ISVS.

Zaměstnanci SZPI, kteří jsou vlastníky procesů, které zpracovávají ISVS jsou funkčními garanty (věcnými správci). Viz interní směrnice pro jednotlivé ISVS.

9.1.4. Poskytování služeb informačních systémů

Funkční část informačního systému, tzn. jaké služby poskytuje a komu je má poskytovat určují jednotliví garanti ve spolupráci s vlastníky daných procesů, a to včetně kontroly dostupnosti, výkonu a kvality.

Všechny smlouvy týkající se ICT mají povinnou součást SLA parametry dle potřeb garantů, a to včetně určení případných sankcí v případě nedodržení.

9.1.5. Útlum, konzervace a ukončení informačních systémů

Případné plánované ukončení provozu je řešeno v jednotlivých smlouvách, a to formou exit plánů.

9.2. Strategie, plánování a organizace řízení informatiky

9.2.1. Zavádění a uplatňování strategického řízení informatiky

Dlouhodobé cíle jsou určeny příručkou jakosti a střednědobou koncepcí SZPI. Cíle v oblasti dlouhodobého řízení ISVS, dle platné legislativy jsou definovány v *Zdrojové tabulky IK v4.xlsx*. Odpovědnost za strategické plánování a implementaci infomačních systémů v souladu s platnou legislativou nese OI OKÚ v závislosti na souhlasném stanovisku nejvyššího vedení SZPI.

9.2.2. Plánování a vyhodnocování činností informatiky

Plánování, cíle a reporting OI OKÚ jsou dány zápisy z porad, plánováním provozního i investičního rozpočtu na základě platných vnitřních předpisů.

9.2.3. Určení odpovědného útvaru pro řízení informatiky

OI OKÚ je aktuálně tvořeno 6 zaměstnanci. Vedoucí OI OKÚ, Manažerem kybernetické bezpečnosti, Architektem kybernetické bezpečnosti – architektem informačního systému SZPI, dvěma informatiky a referentem pro zajištění ekonomických a majetkových procesů. OI OKÚ metodicky řídí jednotlivé správce sítě/informatiky na sedmi krajských pracovištích/inspektorátech.

9.2.4. Nastavení a údržba procesů řízení informatiky

OI OKÚ se v rámci poskytování servisních služeb snaží držet základních best practices dle metodiky ITIL4. V oblasti projektového řízení je využíváno best practices dle PRINCE2. OI OKÚ však aktuálně nedisponuje certifikovaným zaměstnancem v uvedených metodikách.

9.3. Pořízení a změny informačních systémů

9.3.1. Zajištění zdrojů pro pořízení nebo změny IS

Zdroje pro pořízení nebo změny IS se řídí příslušnými VP Odboru personálního, ekonomického a technického. SZPI využívá prostředky z veřejného rozpočtu dle přidělení z nadřízených orgánů. (platí pro provozní i investiční prostředky)

Právní zajištění s ohledem na veřejné zakázky se taktéž řídí příslušnými vnitřními předpisy, které definuje Oddělení veřejných zakázek a smluv (dále OVZS OKÚ).

9.3.2. Identifikace požadavků na IS

O požadavcích na rozšíření nebo úpravu funkcionalit rozhoduje nejvyšší vedení v rámci OP.

9.3.3. Ověřovací koncepty realizovatelnosti

U vybraných informačních systémů (ISVS) má SZPI zajištěno testovací prostředí. Pro systémy pouze v ostrém provozu je po pečlivém naplánování připraven backup plán k zajištění návratu k poslední funkční verzi.

9.3.4. Řízení projektů v oblasti IT

Pro řízení projektů jsou v případě potřeby realizovány pracovní skupiny, jejich vznik a životnost je určována platnými vnitřními předpisy.

9.3.5. Řízení změn IS

Řízení změn je podmíněno rozhodnutím OP, která deleguje poptané úkoly k řešení a realizaci na OI OKÚ.

9.3.6. Vyhodnocování existujících řešení

Při změnách legislativy, popř. na základě požadavků garantů je vždy hledána cesta nejjednoduššího a nejméně nákladného řešení, a to v souladu s již platnou legislativou a požadavky na kybernetickou bezpečnost. Za což je odpovědné OI OKÚ.

9.4. Provoz informačních systémů

9.4.1. Systém řízení provozu IS

Za provoz serverové i informačně-komunikační infrastruktury je v prostředí SZPI odpovědné OI OKÚ.

9.4.2. Monitorování provozu IS

Monitoring provozu IS a celé serverové i informačně-komunikační infrastruktury SZPI je zajišťován v režimu 24/7 OI OKÚ, [redacted]

9.4.3. Správa zdrojů pro provoz IS

Za správu lidských, finančních i technických prostředků pro provoz IS je odpovědné OI OKÚ.

9.4.4. Řízení kontinuity provozu IS

OI OKÚ zajišťuje také nepřetržitý provoz IS v prostředí SZPI, a to na základě určených pohotovostí dle příslušných vnitřních předpisů.

9.4.5. Řízení bezpečnosti provozu IS

Kybernetická bezpečnost je zajištěna dle příslušných vnitřních předpisů. (Řád kybernetické bezpečnosti, Politika kybernetické bezpečnosti atd.).

9.4.6. Využití centrálních sdílených služeb

SZPI využívá hned několik sdílených služeb, v rámci ISVS jsou tyto služby uvedeny u jednotlivých ISVS, viz *Zdrojové tabulky IK v4.xlsx*.

9.5. Poskytování služeb informačních systémů

Všechny aktuálně provozované systémy v SZPI jsou neveřejné, kromě Potravin na pranýři (dále PnP).

PnP je zajišťováno na provozních prostředcích dodavatele, stejně jako Webové stránky. Pro SZPI jsou parametry dostupnosti definovány v rámci SLA na vyžádání skrze helpdesk dodavatele.

9.6. Útlum, konzervace a ukončení informačních systémů

Případné ukončení provozu a konzervace informačních systémů bude řízeno skrze OP a ve spolupráci OI OKÚ s příslušnými dodavateli v souladu s požadavky zákona o kybernetické bezpečnosti, pokud se na ně vztahuje.

Případné přesuny na nové platformy, popř. do nových systémů se budou řídit exit plány u příslušných informačních systémů.

10. SOUVISEJÍCÍ DOKUMENTACE

Zákonné předpisy:

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, v platném znění
- Vyhláška č. 360/2023 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a jakosti informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)
- Zákon č. 264/2025 Sb., o kybernetické bezpečnosti
- Vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („Obecné nařízení EU o ochraně osobních údajů“, také „GDPR“)
- Zákon č. 110/2019 Sb., o zpracování osobních údajů

Normy:

- ČSN EN ISO 9001:2016 - Systémy managementu jakosti - Požadavky
  - SZPI je držitelem certifikátu systému řízení jakosti dle této normy
- ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Požadavky
  - SZPI neplánuje certifikaci systému řízení bezpečnosti informací dle této normy, tato norma slouží jako „best-practices“

Interní předpisová základna SZPI v platném znění:

- Organizační směrnice:
  - [redacted]
- Řády
  - [redacted]
- Strategické dokumenty:
  - [redacted]

- Provozní dokumentace viz manuály (uživatelské a systémové příručky) pro jednotlivé systémy
- Ostatní:

11. PŘÍLOHY

Příloha č. 1 - samostatný dokument Zdrojové tabulky v4.xlsx