Spolufinancováno Evropskou unií

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

PŘÍLOHA Č. 1

TECHNICKÁ SPECIFIKACE INFORMAČNÍHO SYSTÉMU SPRÁVY VOLEB (ISSV)

OBSAH

1. ÚVOD

1.1. CÍL DOKUMENTU

Cílem dokumentu je popis technických požadavků na Informační systém správy voleb („ISSV“). Dokument popisuje projekt v jeho intencích a vztahu k ISSV, dále stanovuje architektonické požadavky, které budou Poskytovatelem dále rozpracovány v rámci dodávky, popisuje požadavky na jednotlivé funkcionality ISSV, systémové vlastnosti ISSV, bezpečnost, shodu s legislativou, požadované testy v rámci dodání, požadované licence k ISSV, vyžadované školení a dodání dokumentace.

Dále dokument uvádí požadavky na řízení projektu Poskytovatelem vč. harmonogramu, který bude dále Poskytovatelem rozpracován v rámci dodávky, respektive projektového řízení dodání ISSV a předimplementační analýzy.

1.2. SOUVISEJÍCÍ DOKUMENTY

Tento dokument je přílohou implementační smlouvy a servisní smlouvy.

Souvisejícím dokumentem je zákon č. 88/2024 Sb., o správě voleb, ve znění pozdějších předpisů, jehož výkon nový ISSV bude zajišťovat.

1.3. POUŽITÉ POJMY A ZKRATKY

Pro účel dokumentu je Zadavatel označován jako „Objednatel“ a Poskytovatel infrastruktury pro fungování ISSV je rovněž označován jako „Poskytovatel infrastruktury Objednatele“. Vítězný uchazeč veřejné zakázky, pro nějž bude tato technická specifikace závazná, je veden jako „Poskytovatel“.

Zkratky užité v tomto dokumentu:

Zkratka	Celý název	Popis
AIFO	Agendový identifikátor fyzické osoby	Technický identifikátor pro účely jednoznačné identifikace fyzické osoby v agendě a jako identifikátor osoby při výměně údajů
AISV	Agendový informační systém vyrozumívání	Informační systém vyrozumívání dle zákona č. 111/2009 Sb., o základních registrech
BSI	Bezvýznamový směrový identifikátor	Identifikátor, který přiděluje NIA každému kvalifikovanému poskytovateli služeb (resp. "uživateli" ve smyslu zákona č. 12/2020 Sb., §12a (1)), na základě kombinace poskytnutých identifikačních údajů fyzické osoby
CAAIS	Centrální autentizační a autorizačního informační systém	Systém autentizace a autorizace uživatelů ISVS, nahrazující JIP/KAAS
CIS	Cizinecký informační systém	Informační systém cizinců podle zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky
CMS/CMS2	Centrální místo sdílených služeb	Komunikační infrastruktura Informačních systémů veřejné správy

ČLH	Člověkohodina	*Jednotka* množství práce vykonané jedním pracovníkem za jednu hodinu
ČSU	Český statistický úřad	Ústřední orgán státní správy ČR
DB	Databáze	Organizovaný soubor strukturovaných informací neboli dat
DC	Datové centrum	Budova, v níž se nachází počítačové servery a další informační technologie
DMZ	Demilitarizovaná zóna	Fyzická nebo logická podsíť, která je z bezpečnostních důvodů oddělena od ostatních zařízení
DPIA	Data Protection Impact Assessment	Posouzení vlivu na ochranu osobních údajů, obsahující popis zpracování údajů, posouzení nezbytnosti a přiměřenosti zpracování, posouzení rizik a stanovení opatření
eGON služby	eGON služby	eGON služby informačního systému základních registrů poskytují údaje vedené v základních registrech a v agendových informačních systémech veřejné správy
EGSB	eGovernment On-Line Service Bus	Informační systém sdílené služby
eIDAS	electronic IDentification, Authentication and trust Services	zkratka pro Nařízení Evropské unie č. 910/2014, o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu
eSSL	Elektronický systém spisové služby	IS pro vedení spisové služby – správu dokumentů úřadu po dobu jejich životního cyklu
EP	Evropský parlament	Jeden ze sedmi orgánů Evropské unie a spolu s Radou Evropské unie přijímá její legislativní akty
FAQ	Frequently Asked Questions	Často kladené dotazy
GIT	GIT	Distribuovaný systém správy verzí (v kontextu dokumentu využit pro zdrojové kódy)
HW	Hardware	Hmotná část ICT, potřebná pro provoz SW
IaaS	Infrastructure As a Service	Distribuční model cloud computingu
ICT	Informační a komunikační technologie	Z anglického "I*nformation and Communication Technologies*" – HW a SW pro komunikaci a sběr, zpracování informací
IČO	Identifikační číslo organizace	Identifikátor právnické osoby

IPMA	International Project Management Association	Projektová metodika
IS	Informační systém	Informační systém – aplikace nebo soubor aplikací využívaných pro podporu procesů, jako prostředek pro sběr, vyhodnocování informací na základě, které lze vytvořit rozhodnutí a případnou interakci.
ISDS	Informační systém datových schránek	Informační systém pro fungování datových schránek a komunikaci přes datové zprávy
ISMS	Systém řízení bezpečnosti informací	Část systému řízení organizace založená na přístupu k rizikům informačního nebo komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat
ISSS	Informační systém sdílené služby	Základní rozhraní propojeného datového fondu veřejné správy
ISSV	Informační systém správy voleb	Výstup projektu – IS pro správu a přípravu voleb
ISVS	Informační systém veřejné správy	Informační systémy dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy
ISZR	Informační systém základních registrů	Informační systém veřejné správy, jehož prostřednictvím je zajišťováno sdílení dat mezi jednotlivými základními registry
IT	Informační technologie	HW a SW pro sběr a zpracování informací
JIP/KAAS	Jednotný identitní prostor/Katalog autentizačních a autorizačních služeb	JIP – zabezpečený adresář orgánů veřejné moci a uživatelských účtů úředník, který je součástí systému Czech POINT. KAAS – rozhraní webových služeb, které umožňují autentizaci uživatelů přistupujících do AIS či ISVS pomocí přihlašovacích údajů v JIP a umožňují editaci údajů subjektů a uživatelských účtů v JIP
ms	Milisekunda	Jednotka času
MVČR	Ministerstvo vnitra České republiky	Ústřední orgán státní správy pro vnitřní věci státu
NIA	Národní identitní autorita	Systém přihlášení a ověření občana.
NIS2	Network and Information Security Directive	Evropská směrnice pro zajištění bezpečnosti ICT
NSESSS	Národní standard pro elektronické systémy spisové služby	Stanovuje podrobné technické požadavky na aplikační

		a byznysové funkce eSSL a evidenci dokumentů
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost	Ústřední správní orgán pro kybernetickou bezpečnost ČR
nZOKB	Nový zákon o kybernetické bezpečnosti	Budoucí zákon o kybernetické bezpečnosti ČR, přejímající evropskou směrnici NIS2
NZSV	Návrh zákona o správě voleb	Připravovaný zákon, jehož výkon bude naplňovat ISSV
ORG	ORG	Převodník identifikátorů dle zákona č. 111/2009 Sb., o základních registrech
OS	Operační systém	SW, který umožňuje správu počítače, řízení hardwaru a běh jiných programů
OU	Obecní úřad	Úřední orgán obecní správy
OVK	Okrsková volební komise	Komise, dbající o řádný průběh hlasování v jednotlivých volebních místnostech
OVM	Orgán veřejné moci	Státní orgán, územní samosprávný celek a fyzická nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy
OWASP	Open Web Application Security Project	Projekt a komunita zabývající se bezpečností webových aplikací
PDF	Portable Document Format	Souborový formát pro ukládání dokumentů nezávisle na softwaru i hardwaru
PDF/A	Portable Document Format Archive	Oficiální archivační verze formátu PDF zaručující zpracování všemi budoucími verzemi softwarových nástrojů
PMI	Project Management Institute	Projektová metodika
POU k zastupování OU	Pověřený obecní úřad	Úřad obce stanovené zákonem (příloha č. 1 k zákonu č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem, ve znění pozdějších předpisů)
PPDF	Propojený datový fond	Tematická oblast tvořená především Informačním systémem základních registrů a Informačním systémem sdílené služby
Prince 2	PRoject IN Control Enviroment	Projektová metodika
Prince 2 Agile	PRoject IN Control Enviroment Agile	Agilní projektová metodika
PSČ	Poštovní směrovací číslo	Číselné označení územního obvodu adresní pošty
REZA	Registr zastupování	Zaváděný referenční zdroj mandátů, umožňující elektronické oprávnění k zastupování
RKL	Registr kandidátních listin	Modul ISSV

ROB	Registr obyvatel	Jeden ze čtyř základních registrů České republiky sloužící k evidenci obyvatel ČR
ROS	Registr osob	Jeden ze čtyř základních registrů České republiky pro evidenci právnických osob, podnikajících fyzických osob a orgánů veřejné moci
RPP	Registr práv a povinností	Jeden ze čtyř základních registrů České republiky pro evidenci podle zákona č. 111/2009 Sb., o základních registrech
RUIAN	Registr územní identifikace adres a nemovitostí	Jeden ze čtyř základních registrů České republiky s informacemi o adresách, územních prvcích, územně evidenčních jednotkách a jejich vzájemných vazbách
SCRUM	SCRUM (skrumáž)	Agilní projektová metodika
SIEM	Security Information and Event Management	Bezpečnostní řešení pro detekci a analýzu hrozeb
SLA	Service-level-agreement	Dohoda o úrovni služeb
SMS	Short message service	Služba zasílání krátkých zpráv mezi mobilními telefony, jinými zařízeními, na pevné telefony nebo přes internet
SPCSS	Státní pokladna centrum sdílených služeb	V kontextu dokumentu Poskytovatel infrastruktury
SSO	Single-sign-only	Autentizace bez nutnosti opakovaného přihlášení uživatelem
SW	Software	Nehmotná část IT, sestávající se z dat a aplikací
UI	User Interface	Uživatelské rozhraní
ÚOOÚ	Úřad na ochranu osobních údajů	Ústřední správní úřad, dohlížející na ochranu soukromí a osobních údajů
VoKB	Vyhláška o kybernetické bezpečnosti	Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
VPN	Virtuální privátní síť	Síť, vytvářející digitální spojení mezi koncovým zařízením a vzdáleným serverem skrze šifrovaný tunel
WBS	Work Breakdown Structure	Dokument rozpadu cíle projektu na aktivity
ZoKB	Zákon o kybernetické bezpečnosti	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů
ZR	Základní registry	Základní (referenční) datový zdroj údajů o subjektech a objektech práva a o výkonu veřejné správy

2. POPIS PROJEKTU

2.1. DŮVOD REALIZACE

Oblast činností úkonů a procesů pro výkon volebního práva je upravena právními předpisy:

- zákon č. 275/2012 Sb., o volbě prezidenta republiky a o změně některých zákonů (zákon o volbě prezidenta republiky), ve znění pozdějších předpisů
- zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů, ve znění pozdějších předpisů
- zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 62/2003 Sb., o volbách do Evropského parlamentu a o změně některých zákonů, ve znění pozdějších předpisů.

Základy právní úpravy voleb jsou stanoveny již v ústavním pořádku, zejména v čl. 5, čl. 16 až 20, čl. 54 až 58 a čl. 102 Ústavy České republiky a v čl. 21, 22 a v čl. 36 odst. 1 a 2 Listiny základních práv a svobod.

Veřejná správa využívá informační systémy použité pro podporu těchto činností a úkonů. Tyto informační systémy jsou nejednotné, decentralizované a roztříštěné, poskytují různou úroveň podpory činností a procesů a mají v odlišné kvalitě implementovány právní předpisy a změny právních předpisů. Možnosti elektronického vyřizování požadavků voličů jsou minimální.

Dopad informačního systému bude celoplošný – bude dostupný pro všechny volební orgány v České republice a pro zastupitelské úřady ČR v zahraničí. Vybrané služby ISSV budou dostupné kandidujícím subjektům (volebním stranám) a občanům (voličům) přímo prostřednictvím ISSV nebo nepřímo přes Portál občana.

Projekt má přinést nápravu neuspokojivého stavu v oblasti správy voleb, kde chybí systematické využití výpočetní techniky a nástrojů eGovernmentu.

Seznamy voličů jsou nyní vedeny jednotlivými obcemi – rozpadají se na více než 6 000 databází. Obce do nich sice čerpají data ze základních registrů, ale ve výsledku je nezřídka vedou papírově, nebo na lokálním disku.

Podávání kandidátních listin nyní nemá jednotná pravidla, která by umožnila jednoduché vytvoření registru kandidátů. Mezi podáním kandidátních listin, vytvořením oline databáze kandidátů a výrobou hlasovacích lístků dnes nastupuje ruční práce Českého statistického úřadu a registračních úřadů, které musejí např. v komunálních volbách zadat do systému data o desetitisících kandidátů.

Neexistuje databáze členů okrskových volebních komisí. Stát nemá spolehlivé informace o obsazování téměř 15 000 komisí vykonávajících státní správu na úseku voleb. Pro starosty obcí je komunikace s volebními stranami mnohdy zbytečně komplikovaná.

V době, kdy každý volič má možnost prokázat svoji identitu pomocí elektronického prostředku, existuje možnost sběru podpisů na podporu kandidatury v zásadě jen v listinné podobě.

Hlavním cílem projektu je vybudování nového informačního systému veřejné správy – Informačního systému správy voleb (ISSV), který se stane novým, jednotným informačním zázemím pro administrativní činnosti ve volebních agendách.

ISSV bude zahrnovat 4 hlavní součásti (moduly):

1. **Jednotný seznam voličů**

Seznam (dále v TS veden jako „seznam voličů“) bude splňovat požadavky na agendový informační systém komunikující se základním registrem obyvatel. Nahradí dnešních cca 6500 „stálých seznamů voličů“, zjednoduší práci obcím a umožní voličům žádat kterýkoli obecní úřad o vydání voličského průkazu nebo změnu volebního okrsku.

2. Registr kandidátních listin

Registr bude postaven na elektronickém formuláři kandidátní listiny. Registr bude databází údajů z kandidátních listin a prezentačním prostředím dokumentů registračního řízení. Spisová služba bude vedena mimo tento systém. Bude umožňovat účastníkům řízení prostřednictvím jejich uživatelského profilu elektronické nahlížení do dokumentů registračního řízení.

3. Registr okrskových volebních komisí

Tento nástroj usnadní komunikaci kandidujících subjektů s obcemi při sestavování okrskových volebních komisí. Delegování členů komisí a jejich následné obesílání obecním úřadem bude elektronické.

4. Nástroj ePetice na podporu kandidatury ve volbách

Informační systém fakultativně umožní také online zakládání a podporu elektronických petic pro nezávislé kandidáty s využitím zaručené elektronické identity.

Cíle projektu jsou v souladu s oblastmi podporovanými výzvou č. 11. Vybudování nového informačního systému ISSV podpoří rozvoj následujících oblastí:

- elektronizace vybraných služeb veřejné správy,
- rozšíření propojeného datového fondu,
- integrace elektronických služeb veřejné správy a informací o službách veřejné správy na portálu gov.cz,
- transakční portálová řešení s využitím zaručené elektronické identity,
- centralizace, standardizace a sdílení elektronických služeb veřejné správy.

Kromě zmiňovaných modulů budou součástí ISSV podpůrné komponenty, související s těmito moduly. Konkrétně se bude jednat o:

1. Komponentu formuláře

Komponenta zajistí vytvoření a publikaci inteligentních elektronických formulářů, vyplnitelných v rámci UI ISSV. Tyto formuláře budou následně vyplnitelné v rámci front-end části ISSV.

Formuláře budou vytvářeny Poskytovatelem a budou součástí dodaného Díla. Další formuláře budou vytvářeny v rámci rozvojových služeb, které jsou definovány v servisní smlouvě a tomto dokumentu.

2. Komponentu statistika

ISSV bude obsahovat analytickou komponentu, která bude fungovat jako business inteligence nadstavba nad daty ISSV. Analytická komponenta bude ve formě přehledných dashboardů zobrazovat statistiky a bude rozšiřitelná o nové předměty zájmu uživatele, analytika.

3. Komponentu administrace

ISSV bude mít k dispozici vlastní administraci pro správu a konfiguraci modularity, funkcí ISSV, správy integrací a databáze.

2.2. CÍL

ISSV se bude skládat ze čtyřech základních modulů:

1. Seznam voličů
2. Registr kandidátních listin
3. Registr členů okrskových volebních komisí
4. Nástroj pro sestavování elektronických petic

Seznam Voličů

Cíle:

- vytvoření jednotného seznamu voličů nahrazujícího dosavadní stálé, zvláštní a dodatkové seznamy
- zrušení místní příslušnosti pro některé úkony, např. pro vydání voličského průkazu
- umožnění přístupu voliče ke svým datům
- umožnění elektronizace úkonů občana ve vztahu k účasti ve volbách, ne však vlastního provedení volby
- snížení chybovosti a snížení administrativní zátěže

Obsah

- Údaje o voličích pro volby do zastupitelstev územních samosprávných celků, Parlamentu České republiky, Evropského parlamentu, volbu prezidenta a referenda.
- Osobní údaje pro Ministerstvo vnitra (správce), obce, zastupitelské úřady, subjekt údajů
- Agregovaná data pro Ministerstvo vnitra, Státní volební komisi, Registrační úřad, Ministerstvo zahraničních věcí, zastupitelské úřady, výrobce hlasovacích lístků, obec, Český statistický úřad.
- Provozní data monitorující činnost systému a přístup k osobním údajům.

Registr kandidátních listin

Cíle:

- vytvoření, podání, kontrola a registrace kandidátních listin,
- příprava podkladů pro výrobu hlasovacích lístků,
- dálkový přístup volební strany k nástrojům pro vytvoření kandidátní listiny,
- dálkový přístup veřejnosti k přehledu volebních stran a náhledům hlasovacích lístků.

Obsah

- obecné údaje o podmínkách registračního řízení,
- údaje z elektronických formulářů uložených v informačním systému volebními stranami,
- údaje z podaných kandidátních listin uvedené včetně osobních údajů kandidátů a zvláštních náležitostí stanovených zákonem o volbách,
- údaje o průběhu a výsledku registračního řízení a obsah registrovaných kandidátních listin,
- údaje o historii přístupů a změn v obsahu registru kandidátních listin,
- datové úložiště s elektronickými obrazy dokumentů registračního řízení,
- výstupy pro přípravu a výrobu hlasovacích lístků a náhledy hlasovacích lístků.

Registr členů okrskových volebních komisí

Hlavním cílem registru členů okrskových volebních komisí je

- usnadnění komunikace kandidujících subjektů s obcemi při delegování členů okrskových volebních komisí a
- poskytnutí nástroje pro ustanovení okrskových volebních komisí.

Tento registr musí být propojen s registrem kandidátních listin, neboť musí být zaručena kontrola inkompatibility kandidáta s členstvím v okrskové volební komisi pro okrsek, kde kandiduje. Jiné nepřípustné kombinace rolí nebyly identifikovány.

Nástroj pro sestavování elektronických petic

Nástroj pro sestavování elektronických petic, dále jen ePetice, slouží volebním subjektům, jejichž kandidatura vyžaduje podle zákona podporu voličů formou petice:

- Umožňuje online zakládání a podporu elektronických petic s využitím zaručené elektronické identity.
- Kandidát uděluje souhlas se založením petice na svoji podporu (ověřený podpis), nelze založit petici bez souhlasu kandidáta, to neplatí pro sdružení nezávislých kandidátů.
- Kandidát má právo zrušit petici na svoji podporu.
- Pro jedny volby nelze založit více petic, petice obsahuje jedinečný osobní identifikátor kandidáta nebo jedinečný název volební strany skupiny nezávislých kandidátů.

Komponenta formuláře

Komponenta zajistí vytvoření a publikaci elektronických formulářů, vyplnitelných v rámci UI ISSV. Tyto formuláře budou následně vyplnitelné v rámci front-end části modulů ISSV.

- Umožňuje online zakládání elektronických formulářů v rámci UI portálu s využitím zaručené elektronické identity.
- Zajistí přenos informací z formuláře do DB ISSV
- Zajišťuje předvyplnění údajů z dostupných údajů z ISZR
- Kontroluje korektní vyplnění formuláře s využitím šablon

Komponenta statistika

ISSV bude obsahovat analytickou komponentu, která bude fungovat jako business inteligence nadstavba nad daty ISSV. Analytická komponenta bude ve formě přehledných dashboardů zobrazovat statistiky a bude rozšiřitelná o nové předměty zájmu uživatele, analytika.

- Zajistí analýzu provozního chování a využívání jednotlivých registrů
- Umožní vyhodnocování procesů a datových výstupů
- Poskytne srovnání statistik porovnáváním mezi jednotlivými volbami, referendy
- Umožní definování vlastních analytických výstupů a pohledů na datové sady v rámci datového skladu
- Zajistí vytváření open-dat

Komponenta administrace

ISSV bude mít k dispozici vlastní administraci pro správu a konfiguraci modularity, funkcí ISSV, správy integrací a databáze.

2.3. POŽADOVANÉ VÝSTUPY

ISSV zahrnuje čtyři hlavní součásti:

1. Seznam voličů
    a. vytvoření jednotného seznamu voličů nahrazujícího dosavadní stálé, zvláštní a dodatkové seznamy
    b. zrušení místní příslušnosti pro některé úkony, např. pro vydání voličského průkazu
    c. umožnění přístupu voliče ke svým datům
    d. umožnění elektronizace úkonů občana ve vztahu k účasti ve volbách, ne však vlastního provedení volby

2. Registr kandidátních listin
    a. vytvoření, podání, kontrola a registrace kandidátních listin,
    b. příprava podkladů pro výrobu hlasovacích lístků,
    c. dálkový přístup volební strany k nástrojům pro vytvoření kandidátní listiny,
    d. dálkový přístup veřejnosti k přehledu volebních stran a náhledům hlasovacích lístků.

3. Registr členů okrskových volebních komisí
    a. usnadnění komunikace kandidujících subjektů s obcemi při delegování členů okrskových volebních komisí
    b. poskytnutí nástroje pro ustanovení okrskových volebních komisí.

4. Nástroj pro sestavování elektronických petic
    a. Umožnění online zakládání a podpory elektronických petic s využitím zaručené elektronické identity.
    b. Kandidát uděluje souhlas se založením petice na svoji podporu (ověřený podpis), nelze založit petici bez souhlasu kandidáta, to neplatí pro sdružení nezávislých kandidátů.
    c. Kandidát má právo zrušit petici na svoji podporu.
    d. Pro jedny volby nelze založit více petic, petice obsahuje jedinečný osobní identifikátor kandidáta nebo jedinečný název volební strany skupiny nezávislých kandidátů.

Dále budou poskytnuty podpůrné komponenty a funkce, mj. komponenta formuláře, komponenta administrace, komponenta statistika a integrační rozhraní – viz. kapitola Požadavky na architekturu ISSV.

Důležitou součástí ISSV je veřejné rozhraní umožňující přístup občanů k elektronickému podání a zajišťující informovanost široké veřejnosti. Díky svým komponentům ISSV rozšiřuje také možnosti elektronické komunikace mezi volebními orgány, voliči a kandidáty či politickými stranami. ISSV sjednocuje a centralizuje správní procesy volební agendy, přičemž přináší vyšší efektivitu v oblasti sdílení a zpracování dat a snižuje tak riziko duplicit a nesrovnalostí.

1. ISSV vznikne ucelená databáze údajů potřebných pro vedení a správu volební agendy, což umožní uživatelům vyhledávání a zadávání dat centrálně za použití IS.
2. Systém má vysoký potenciál pro urychlení a usnadnění komunikace mezi dotčenými volebními orgány o zapisovaných skutečnostech a tím přispěje mimo jiné ke zvýšení aktuálnosti dat (např. elektronické podávání kandidátních listin a jejich registr, centrální seznam voličů, registr okresních volebních komisí a nástroj e-petice).
3. Dále ISSV sníží zátěž vzniklou místní příslušností úřadů v oblasti volební agendy a zejména voličům umožní vyřídit náležitosti spojené s volbami na kterékoliv obecním úřadě, bez ohledu na jejich místní příslušnost (např. vyřízení voličského průkazu bude nově možné na kterémkoli obecním úřadě).
4. Obecně nový centrální systém přispěje k automatizaci úkonů činěných v oblasti správy volební agendy.

Kromě těchto výstupů bude součástí výstupu Díla poskytnutí souvisejících služeb, především:

- Projektového řízení dodání, součinnost s Objednatelem a dalšími zainteresovanými stranami projektu
- Vytvoření předimplementační analýzy nového IS
- Otestování řešení, odstranění vad
- Vytvoření vývojového prostředí ISSV v prostředí Poskytovatele
- Migrace ISSV do testovacího, preprodukčního a produkčního prostředí za součinnosti Objednatele, Poskytovatele infrastruktury Objednatele, potažmo technických správců cílových prostředí
- Návrh, vytvoření a naplnění databáze IS
- Realizace integrací
- Vytvoření systémové, administrátorské a uživatelské dokumentace
- Školení Objednatele
- Předání zdrojových kódů
- Předání licencí
- Asistence při pilotním provozu
- Součinnost při metodické podpoře uživatelů

Dalšími službami po dodání a akceptaci ISSV bude poskytnutí servisních služeb, spočívajících se v zajištění funkčnosti a aktuálnosti ISSV, rovněž s ohledem na aktuální legislativu a s důrazem na zajištění kybernetické bezpečnosti ISSV.

Součástí servisní smlouvy bude závazek poskytnutí rozvojových prací na ISSV, spočívajících v rozvoji funkcionality, součástí je mj. závazek vytváření či úpravy elektronických formulářů na požadavek Objednatele. Tyto služby budou poskytovány na rámcovou smlouvu. V případě, že nedojde k uzavření servisní smlouvy, bude Poskytovatelem poskytnuta dvouletá záruka na dodaný systém a jeho funkcionality, detail vč. SLA je uveden ve smlouvě.

3. POŽADAVKY NA ARCHITEKTURU ISSV

ISSV je informačním systémem veřejné správy a je součástí kritické infrastruktury státu

3.1. BUSINESS ARCHITEKTURA – POKRYTÍ PROCESŮ ISSV

Business architektura uvedená v této kapitole nezahrnuje činnosti, procesy, funkce a služby, které jsou nutné pro zajištění požadavků právních předpisů, ale jsou vykonávány mimo informační systém ISSV nebo portál občana. Důležitou součástí ISSV je **veřejné rozhraní** umožňující přístup občanů k elektronickému podání a zajišťující informovanost široké veřejnosti, včetně zveřejňování zákonem předepsaných dokumentů v jednotlivých fázích volebního procesu. Veškeré uživatelské rozhraní systému bude v českém jazyce s následujícím upřesněním – uživatelské rozhraní přihlášeného voliče bude v českém a anglickém jazyce. Veřejná část ISSV bude mít uživatelské rozhraní rovněž dvoujazyčné – v českém a anglickém jazyce. Tímto způsobem bude zajištěna podpora uživatelů, voličů ze zemí EU.

Služby a funkce business architektury jsou rozděleny na úrovni aktérů. Informace určené pro veřejnost budou k dispozici na veřejném rozhraní ISSV, které bude dostupné i z portálu občana. Tyto informace budou přístupné i veřejnosti bez autentizace.

Pro autentizovanou veřejnost zajistí portál občana informační rozcestník. Informační rozcestník zajistí pro definované životní situace, které budou podporovány ISSV přesměrování uživatele na konkrétní rozhraní určené k řešení této situace.

Služby elektronického podání budou přístupné pro autentizovanou veřejnost pomocí inteligentních formulářů na veřejném rozhraní ISSV. Vlastní úkon bude uživatelem potvrzen prostřednictvím autorizace digitálního podání. ISSV vydá v souladu se zněním Zákona 12/2020 Sb. O právu na digitální služby vydá osvědčení o digitálním úkonu, které předá, nebo zašle do datové schránky ISDS podle předané preference uživatele. Prostřednictvím veřejného rozhraní ISSV pro autentizované uživatele budou poskytovány i služby vyžadující využití zjišťování dalších informací z propojeného datového fondu a tím i komplexnějších integrací na Základní registr osob (ROS), Základní registr územní identifikace adres a nemovitostí (RUIAN), Registr zastupování (REZA), nebo služby vyžadující realizaci komplexního procesu a tím i opakovaných operací s daty.

Pro odbornou veřejnost bude ISSV poskytovat grafické uživatelské rozhraní. Bude umožněno využití integrací do propojeného datového fondu, realizace komplexních procesů a opakovaných operací s daty. Služby a funkce budou seskupeny pro jednotlivé registry a podle aktérů, Statistika a administrace budou logicky odděleny do samostatných rozhraní. Bude kladen důraz na přehlednost a srozumitelnost uživatelského rozhraní systému.

Samostatné rozhraní bude vytvořeno pro správce. Toto rozhraní umožní realizaci iniciačních kroků, správu číselníků, správu integrací (integrace se systémem základních registrů, s informačním systémem sdílené služby (ISSS), s informačním systémem datových schránek (ISDS), integrace se systémy spisové služby s využitím národního standardu NSESSS), vyvolání jednorázových a nastavení opakovaných aktualizací dat, nastavení a kontrolu milníků klíčových procesů, správu notifikací.

Seznam voličů bude sloužit pro vytvoření jednotného seznamu voličů a umožní realizovat zrušení místní příslušnosti pro některé úkony. Seznam voličů bude obsahovat údaje o voličích pro volby do zastupitelstev územních samosprávných celků, Parlamentu České republiky, Evropského parlamentu, volbu prezidenta a referenda. Seznam voličů musí automaticky vyhodnotit právo volit a vytvořit výstupy ze seznamu voličů s požadovanými údaji požadovanými právními předpisy. Parametry seznamu jsou určeny druhem voleb, volebními obvody, kolem voleb, datem konání voleb. Seznam voličů je

ovlivněn i pobytem v zařízení, kdy jsou nastaveny procesy, aby bylo umožněno volit i voličům, kteří se nemohou dostavit. do volební místnosti.

Registr kandidátních listin bude databází údajů z kandidátních listin a prezentačním prostředím dokumentů registračního řízení. Bude umožňovat účastníkům řízení prostřednictvím jejich uživatelského profilu elektronické nahlížení do dokumentů registračního řízení.

Registr členů okrskových volebních komisí umožní elektronickou komunikaci kandidujících subjektů s obcemi při delegování členů komisí a sestavování okrskových volebních komisí.

Nástroj ePetice umožní také zakládání a podporu elektronických petic pro nezávislé kandidáty s využitím zaručené elektronické identity.

Informační systém bude obsahovat společný nástroj Statistika, který umožní analýzu provozního chování a využívání jednotlivých registrů a také vyhodnocování procesů a datových výstupů a jejich charakteristik a také jejich porovnávání mezi jednotlivými volbami, referendy a peticemi, a to z pohledů časového, množstevního, geografického, věkového, případně dalších. Nástroj umožní uživatelům definování vlastních analytických výstupů a pohledů na datové sady v rámci datového skladu. Jedním z výstupů statistiky budou i otevřená data. Ve formátu otevřených dat budou publikovány informace o volbách, statistické informace o volebních územích atd., bude upřesněno v rámci úvodní analýzy.

Systém bude také poskytovat společné sdílené služby, které budou plnit požadavky právních předpisů v oblasti:

- Vytvoření osvědčení o digitálním úkonu, včetně pečetě
- Zaznamenávání činnosti systému a aktérů
- Monitorování a poskytování informací pro vyhodnocení provozních charakteristik a SLA
- Zaznamenávání auditních událostí a předávání relevantních auditních událostí bezpečnostnímu dohledu
- Zálohování systému a dat

Poskytování služeb a jejich požadovaná kvalita bude podporována poskytování služeb provozní podpory.

Tabulka: katalog prvků business architektury

Typ prvku	Jméno prvku	Popis prvku
Business Actor	Aktér - Volič	Aktér volič občan
Business Actor	Aktéři ePetice	Aktér uživatelé ePetice
Business Actor	Kandidát	Aktér druh kandidáta
Business Actor	Krajský úřad	krajský úřad, Magistrát hlavního města Prahy (dále jen "Krajský úřad"),
Business Actor	Ministerstvo vnitra	Aktéři a role MVČR
Business Actor	Obecní úřad	Registru členů OVK pro účely nastavení rozsahu přístupových oprávnění volebních stran. Je potřeba zajistit, aby v registru členů OVK neměla táž volební strana přístup k nominaci do téže OVK vícekrát.
Business Actor	Ostatní Aktéři ISSV	Aktéři a role IS Správy voleb. Úřad pro dohled nad hospodařením politických stran a politických hnutí (registrační úřad už nebude muset sdělovat

		adresně Úřadu, kdo podal kandidátní listinu).
Business Actor	Politická strana	Zmocněnci volebních stran (v některých případech i volební strany přímo) ke svému podání. Mají právo: nahlížení na stav podání, avíza, výzvy registračního úřadu.
Business Actor	Pověřený obecní úřad	Registru členů OVK pro účely nastavení rozsahu přístupových oprávnění volebních stran. Je potřeba zajistit, aby v registru členů OVK neměla táž volební strana přístup k nominaci do téže OVK vícekrát.
Business Actor	Registrační úřad	Aktéři a role Registrační úřady
Business Actor	Státní volební komise	Vykonává také roli Registračního úřadu pro určité typy voleb
Business Actor	Systém	Startování a aktualizace kontrolních procesů
Business Actor	Výrobce hlasovacích lístků	Aktéři a role výrobců hlasovacích lístků
BusinessActor	Zastupitelský úřad a konzulátský úřad	zastupitelský úřad a konzulární úřad České republiky, s výjimkou konzulárního úřadu vedeného honorárním konzulárním úředníkem, (dále jen "zastupitelský úřad"),
Business Actor	Úřad pro dohled nad hospodařením politických stran a politických hnutí	Role - Úřad pro dohled nad hospodařením politických stran a politických hnutí
Business Actor	Český statistický úřad (ČSU)	Aktéři a role Českého statistického úřadu (ČSU)

V následujících schématech je zobrazeno přiřazení Aktérů k procesům.

Schéma: Aktér Volič

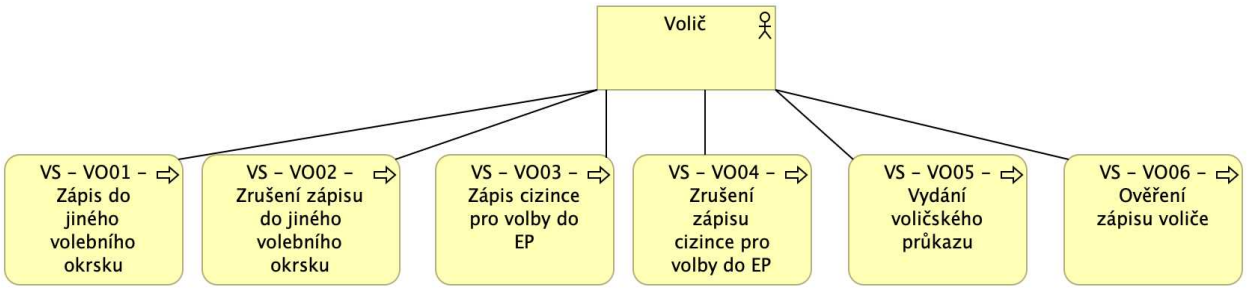


Schéma: Aktér Veřejnost

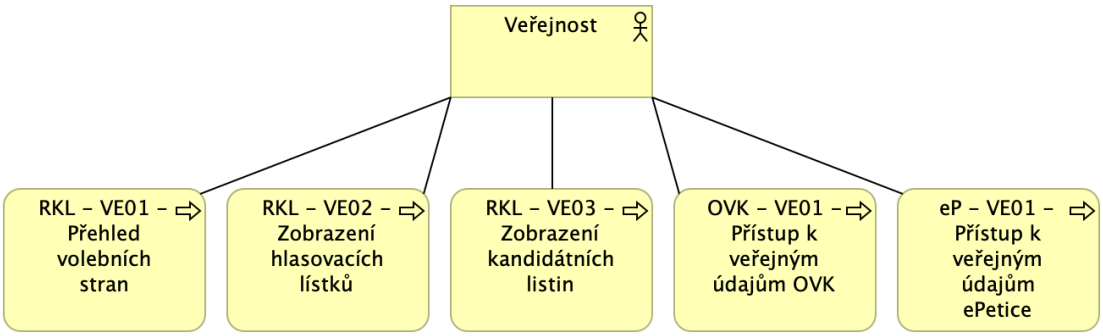


Schéma: Aktér Zájemce

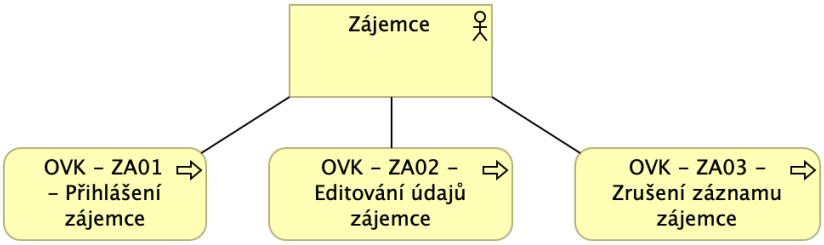


Schéma: Aktér Petent

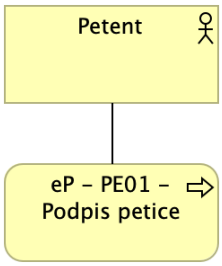


Schéma: Aktér Pověřená osoba

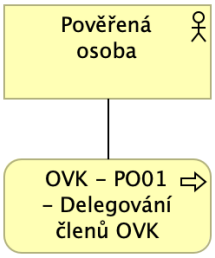


Schéma: Aktér Statutární orgán

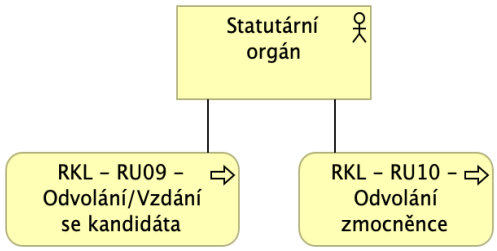


Schéma: Aktér Zmocněnec

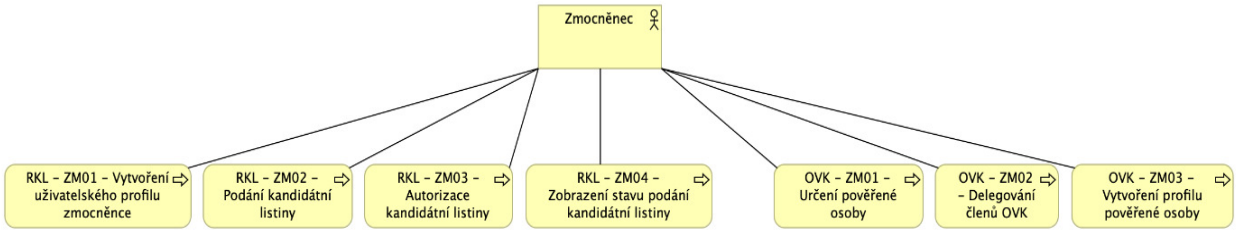


Schéma: Aktér Zakladatel petice

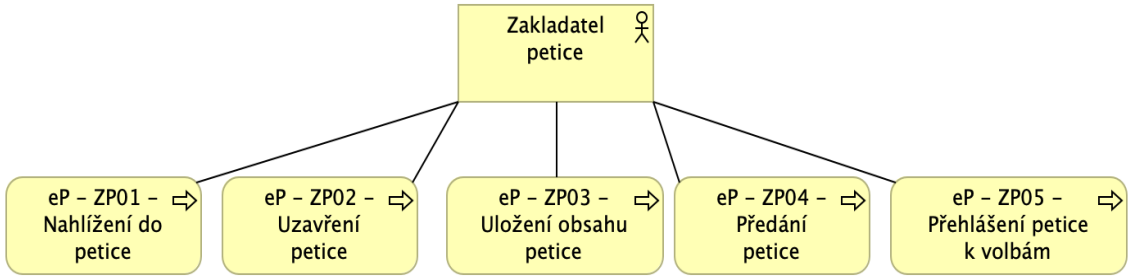


Schéma: Aktér Obec

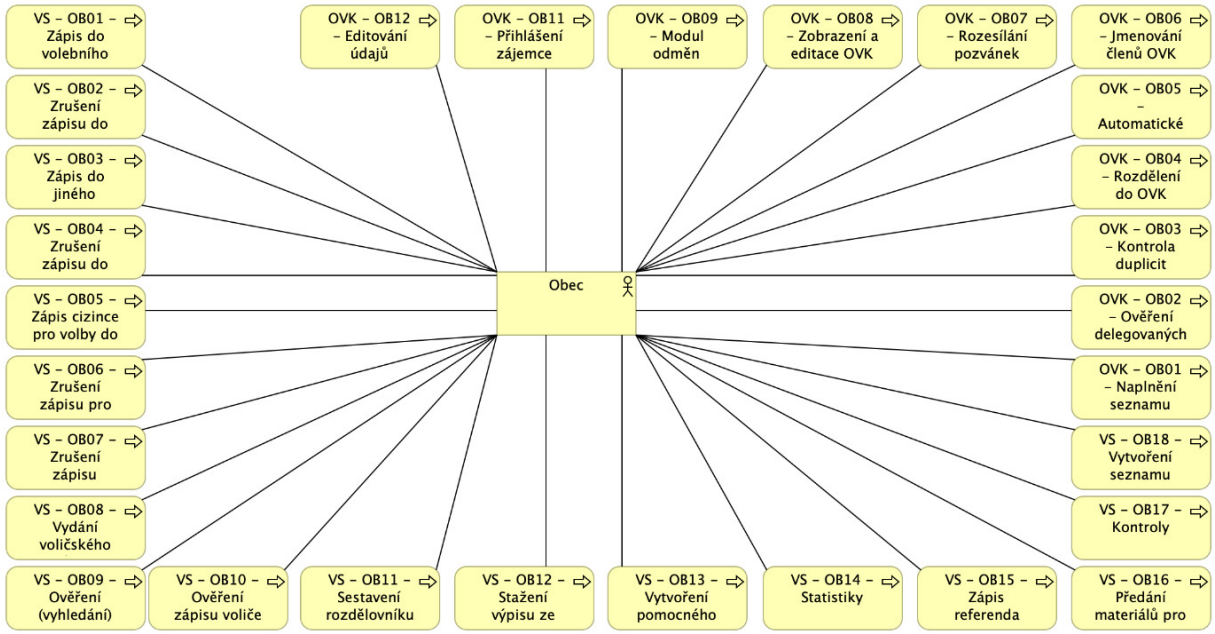


Schéma: Aktér Kraj

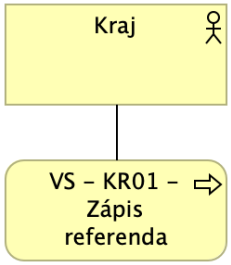


Schéma: Aktér Ministerstvo vnitra

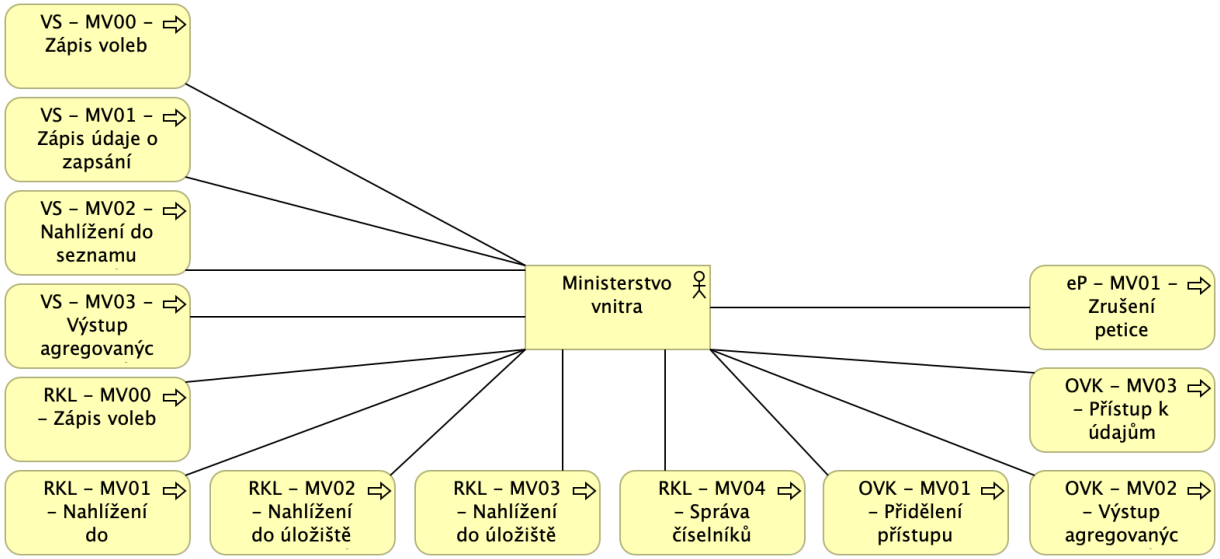


Schéma: Aktér Zastupitelský úřad

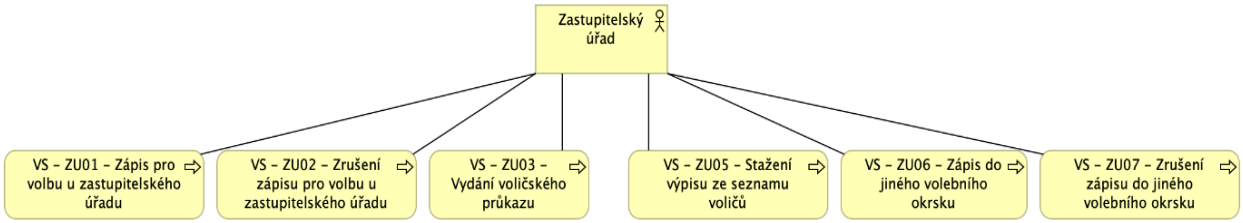


Schéma: Aktér Kontaktní místo veřejné správy

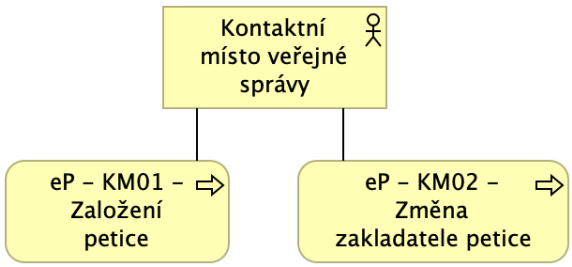


Schéma: Aktér Registrační úřad

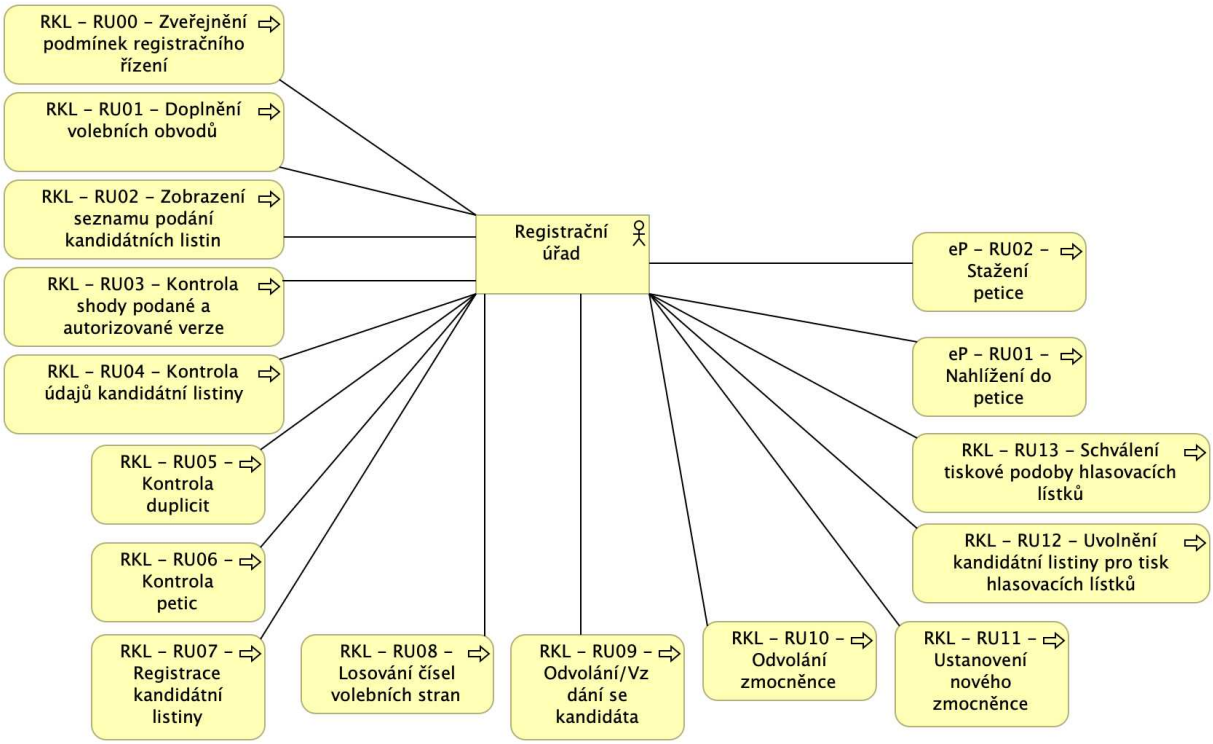


Schéma: Aktér Úřad pro dohled nad hospodařením politických stran a politických hnutí

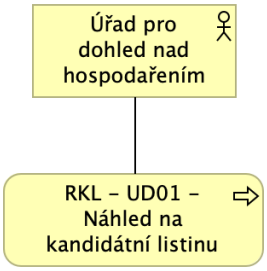


Schéma: Aktér Výrobce hlasovacích lístků

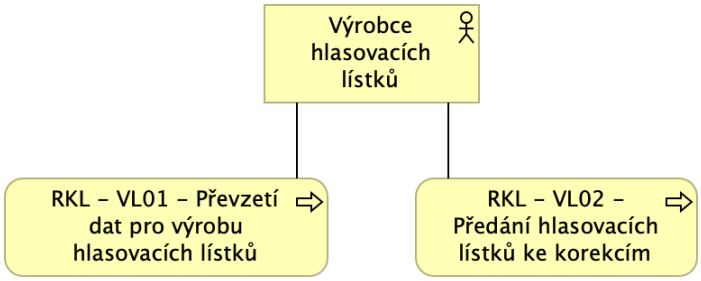


Schéma: Aktér Český statistický úřad

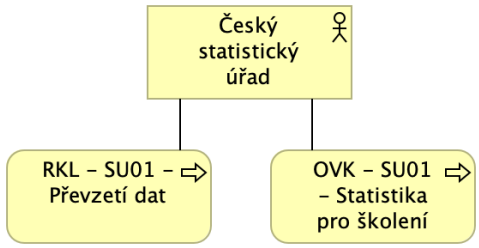
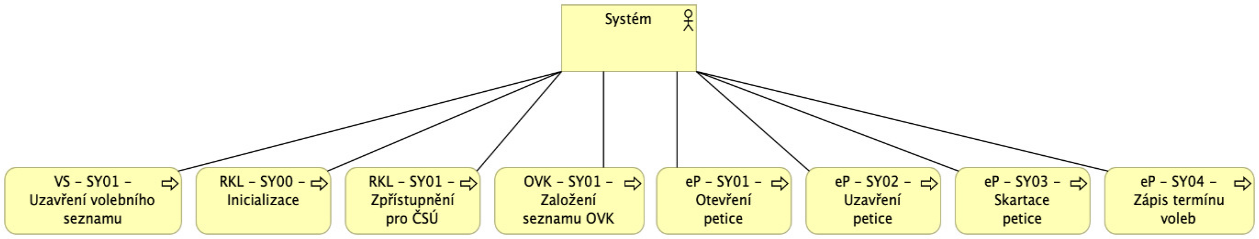


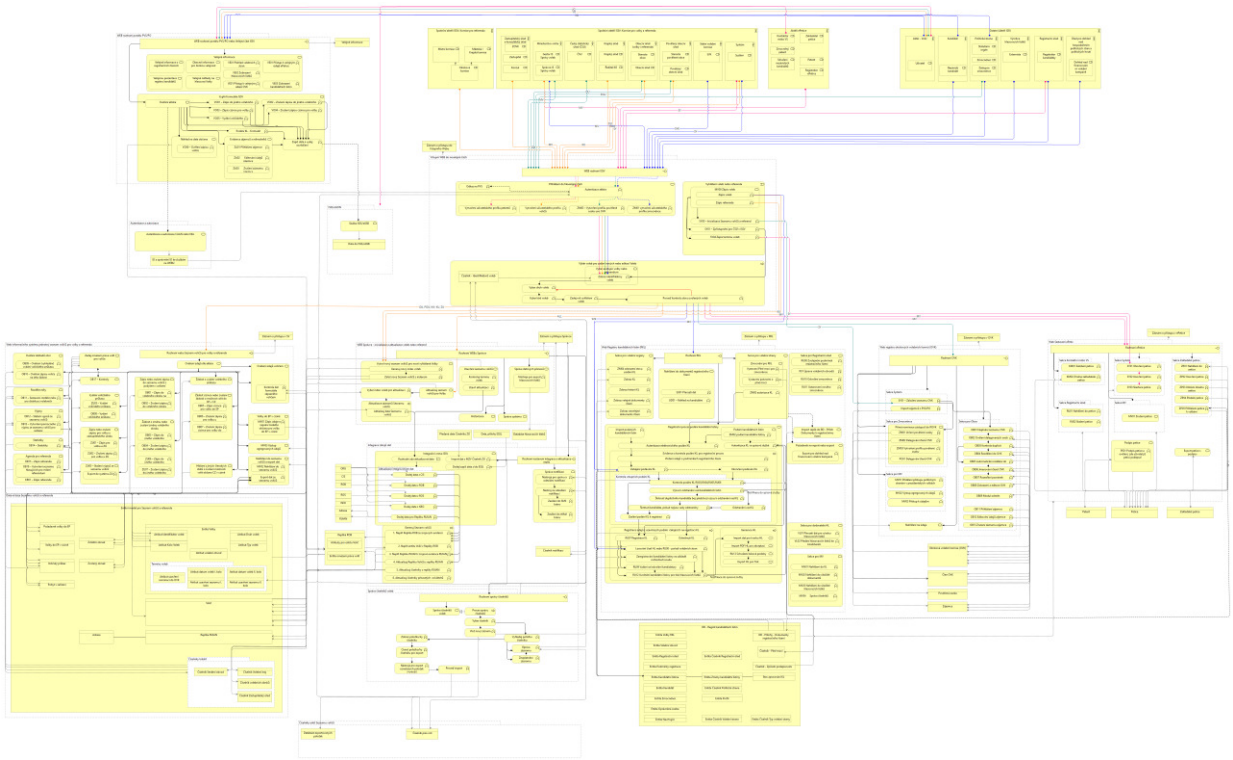
Schéma: Aktér Systém



Uvedené procesy jsou dokumentovány jako činnosti v kapitole 4 tohoto dokumentu.

Celkový přehled business architektury je uveden na následujícím schéma.

Schéma: Business architektura

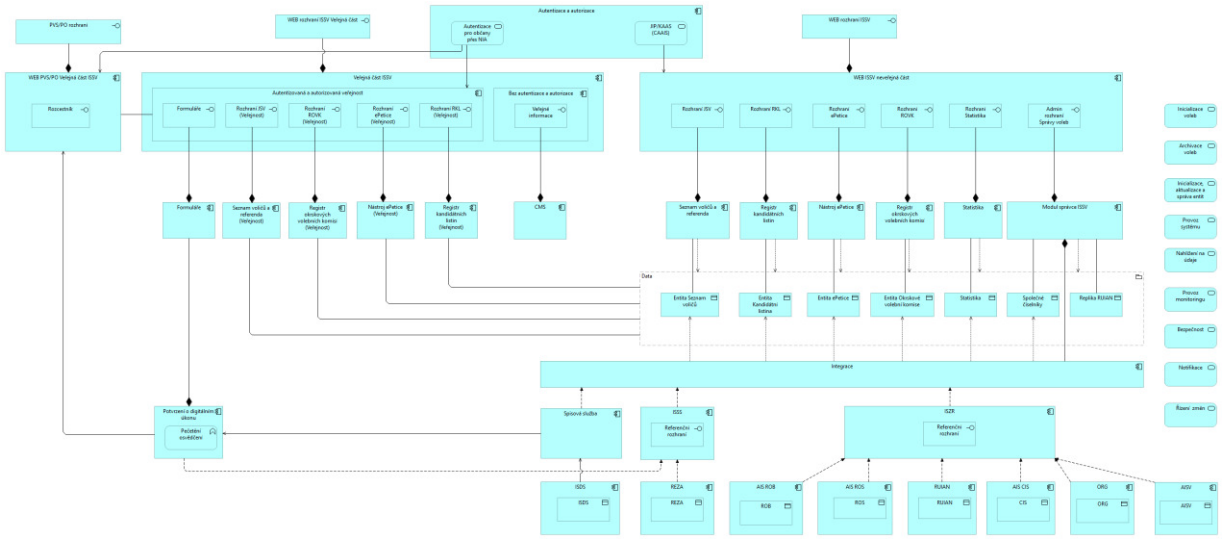


3.2. APLIKAČNÍ ARCHITEKTURA

Aplikační architektura ISSV bude obsahovat vrstvu prezentační, rozhraní, aplikační logiku a datovou vrstvu.

Z důvodu sezónnosti poskytovaných služeb je požadováno systém rozdělit na jednotlivé registry, administrační, servisní a analytické části tak aby bylo možné horizontální škálovat tyto části na sobě nezávisle a zároveň výrazně. Z těchto důvodů je požadováno vytvoření nativně cloudové architektury.

Schéma: Aplikační architektura



Typ prvku	Jméno prvku	Popis prvku
Application component	WEB PVS/PO Veřejná část ISSV	Komponenta mimo systém ISSV. Obsahuje informace pro občany, možnost získat osvědčení o provedených úkonech a Rozcestník ke konkrétním úkonům a informacím v rámci ISSV. Při přechodu na ISSV bude využito principu SSO.
Application component	Autentizace a autorizace	Komponenta mimo systém ISSV. Představuje služby autentizace a případně autorizace reprezentované systém NIA a JIP/KAAS(CAAIS).
Application component	Veřejná část ISSV	Portál pro veřejnost zastřešuje část pro autentizovanou a část pro neautentizovanou veřejnost. Směrem k uživatelům je reprezentován webovým rozhraním pro veřejnost.
Application component	Autentizovaná a autorizovaná veřejnost	Webová aplikace/portál pro autentizovanou veřejnost poskytuje pro veřejnost autentizovanou prostřednictvím NIA a autorizovanou pro definované funkce zejména v RKL rozhraní pro získávání informací a formuláře umožňující elektronické podání.
Application component	Bez autentizace a autorizace	Webová aplikace/portál pro anonymní uživatele poskytuje obecné informace a pokyny v souvislosti se

Typ prvku	Jméno prvku	Popis prvku
		službami a procesy informačního systému.
Application component	WEB ISSV neveřejná část	Webová aplikace/portál pro interní uživatele zpřístupňuje rozhraní pro uživatele autentizované prostřednictvím JIP/KAAS (CAAIS) poskytující přístup k funkcím podporujícím konkrétní činnosti jednotlivých rolí v agendě.
Application component	Formuláře	Elektronické interaktivní formuláře slouží pro automatizaci interakce veřejnosti se službami eGovernmentu. Formulář je typ strukturovaného dokumentu, který umožňuje uživatelům zadávat a odesílat data prostřednictvím webového rozhraní. Oproti běžným elektronickým dokumentům, jako jsou textové soubory nebo PDF, elektronické formuláře nabízejí interaktivitu a budou předvyplňovat data prostřednictvím integrace na PPDF a základní registry.
Application component	Seznam voličů a referenda (Veřejnost)	Realizuje aplikační logiku poskytující API funkce pro přístup k seznamu voličů a k referendům pro veřejnost.
Application component	Registr okrskových volebních komisí (Veřejnost)	Realizuje aplikační logiku poskytující API funkce pro přístup k registru okrskových volebních komisí pro veřejnost.
Application component	Nástroj ePetice (Veřejnost)	Realizuje aplikační logiku poskytující API funkce pro přístup k ePeticím pro veřejnost.
Application component	Registr kandidátních listin (Veřejnost)	Realizuje aplikační logiku poskytující API funkce pro přístup k registru kandidátních listin pro veřejnost.
Application component	Seznam voličů a referenda	Realizuje aplikační logiku poskytující API funkce pro přístup k seznamu voličů a k referendům pro interní uživatele.
Application component	Registr okrskových volebních komisí	Realizuje aplikační logiku poskytující API funkce pro přístup k registru okrskových volebních komisí pro interní uživatele.
Application component	Nástroj ePetice	Realizuje aplikační logiku poskytující API funkce pro přístup k ePeticím pro interní uživatele.
Application component	Registr kandidátních listin	Realizuje aplikační logiku poskytující API funkce pro přístup k registru kandidátních listin pro interní uživatele.

Typ prvku	Jméno prvku	Popis prvku
Application component	Statistika	Umožňuje definovat vlastní pohledy na předpřipravené datové sady. Tyto datové sady naplní datový sklad pomocí ETL nebo obdobného nástroje z dat jednotlivých registrů.
Application component	Modul správce ISSV	Aplikace pro správce umožní realizovat administraci a správu informačního systému v oblastech: • Správa entit • Archivace • Inicializace • Notifikace • Aktualizace dat • Správu plánovaných úloh
Application component	Potvrzení o digitálním úkonu	Komponenta realizující vytvoření a předání osvědčení o digitálním úkonu dle zákona č. 12/2020 Sb., o právu na digitální služby.
Application component	Integrace	Realizuje aplikační rozhraní k externím informačním systémům. Toto aplikační rozhraní konzumuje služby spisové služby, ISSS, ISRZ a poskytuje služby ISSS, využitelné i pro výdej dat a seznamů. Alternativní možnosti datového výdeje zmapuje přeimplementační analýza.
Application component	Spisová služba	Komponenta mimo systém ISSV. Poskytuje rozhraní NSESSS pro čtení i zápis dokumentů.
Application component	ISSS	Komponenta mimo systém ISSV. Informační systém sdílené služby dle zákona č. 111/2009 Sb., o základních registrech.
Application component	ISZR	Komponenta mimo systém ISSV. Informační systém základních registrů dle zákona č. 111/2009 Sb., o základních registrech.
Application component	ISDS	Komponenta mino systém ISSV. Informační systém datových schránek
Application component	REZA	Komponenta mino systém ISSV. Registr zastupování.
Application component	AIS ROB	Komponenta mimo systém ISSV. Základní registr obyvatel dle zákona č. 111/2009 Sb., o základních registrech.
Application component	AIS ROS	Komponenta mimo systém ISSV. Základní registr osob dle zákona č. 111/2009 Sb., o základních registrech.
Application component	RUIAN	Komponenta mimo systém ISSV. Základní registr územní identifikace,

Typ prvku	Jméno prvku	Popis prvku
		adres a nemovitostí dle zákona č. 111/2009 Sb., o základních registrech.
Application component	AIS CIS	Komponenta mimo systém ISSV. Informační systém cizinců podle zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky.
Application component	ORG	Komponenta mimo systém ISSV. Převodník identifikátorů dle zákona č. 111/2009 Sb., o základních registrech.
Application component	AISV	Komponenta mimo systém ISSV. Informační systém vyrozumívání dle zákona č. 111/2009 Sb., o základních registrech.
Data object	Entita seznam voličů	Zajišťuje perzistenci dat pro seznam voličů a referenda.
Data object	Entita Kandidátní listiny	Zajišťuje perzistenci dat pro registr kandidátních listin.
Data object	Entita ePetice	Zajišťuje perzistenci dat pro nástroj ePetice.
Data object	Entita Okrskové volební komise	Zajišťuje perzistenci dat pro registr okrskových volebních komisí.
Data object	Statistika	Datový sklad skládající se z datových sad pro vytváření datových pohledů a výstupů na základě definovatelných hledisek.
Data object	Společné číselníky	Zajišťuje perzistenci dat pro číselníky včetně jejich předchozích údajů.
Data object	Replika RUIAN	Lokální aktualizovaná kopie RUIAN obsahující historii údajů pro zajištění integrity dat v průběhu a po volbách.
Application service	Inicializace voleb	Reprezentuje aplikační službu, kterou zajistí ISSV.
Application service	Archivace voleb	Reprezentuje aplikační službu, kterou zajistí ISSV.
Application service	Inicializace, aktualizace a správa entit	Reprezentuje aplikační službu, kterou zajistí ISSV.
Application service	Provoz systému	Reprezentuje aplikační službu, kterou zajistí ISSV. Zajištění definovaných SLA na úrovni aplikační architektury, která zahrnuje aplikační a platformový software je v kompetenci Poskytovatele ISSV.
Application service	Nahlížení na údaje	Reprezentuje aplikační službu, kterou zajistí ISSV.
Application service	Provoz monitoringu	Reprezentuje aplikační službu, kterou zajistí ISSV. Monitoring stavu komponent aplikační architektury je nezbytný pro zajištění provozu a vyhodnocování SLA.

Typ prvku	Jméno prvku	Popis prvku
Application service	Bezpečnost	Reprezentuje aplikační službu, kterou ISSV umožní splnit definované požadavky na bezpečnost systému podle provedené analýzy rizik a v souladu s právními předpisy o kybernetické bezpečnosti. Dále IS implementuje zaznamenávání událostí tak, aby je bylo možné z jednoho místa v každém DC předávat k vyhodnocení na SIEM službu poskytovanou provozovatelem DC.
Application service	Notifikace	Reprezentuje aplikační službu, kterou zajišťuje ISSV.
Application service	Řízení změn	Reprezentuje aplikační službu, kterou architektura ISSV umožní realizovat. Aplikační komponenty musí pomocí dokumentace a řízení API, řízením a dokumentací verzí a dostupností repository balíčků a kontejnerů správně reagovat na požadavky ITIL procesů týkající se řízení změn a problémů v systému.

3.3. APLIKAČNÍ ARCHITEKTURA – INTEGRACE

Pro komunikaci s agendovými informačními systémy veřejné správy bude ISSV využívat Referenční rozhraní v souladu s jeho definicí zakotvenou zejména v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů a zákoně č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. Využívání údajů prostřednictvím referenčního rozhraní je vždy realizováno výhradně na základě příslušných oprávnění evidovaných v registru práv a povinností (RPP) definovaných při ohlášení Agendy v AIS Působnostním.

ISSV realizovat využívání údajů ze základních registrů:

- S ohledem na oprávnění k přístupu k údajů v základních registrech, podle ohlášení jednotlivých agend v RPP, s využitím služeb vnějšího rozhraní ISZR
- Realizují se také služby notifikací a aktualizací údajů základních registrů s využitím služeb vnějšího rozhraní ISZR

Základní pravidla pro využívání referenčního rozhraní, které bude ISSV splňovat

- Dodržovat vyhlášky k zákonu 365/2000 Sb., především o technických a funkčních parametrech připojení k referenčnímu rozhraní
- Každý systém přistupující k referenčnímu rozhraní musí prokazovat svoji "identitu" prostřednictvím systémového certifikátu vydaného Certifikační autoritou ve správě DIA
- Při výměně údajů o subjektech práva či objektech územní identifikace se ověřuje, zda tyto subjekty (ROB, ROS) či objekty (RÚIAN, RPP) jsou uvedeny v základních registrech (ověření referenční vazby)

- OVM, které požaduje údaje o konkrétním subjektu, je zodpovědné za jeho řádné ztotožnění ve své agendě, tj. uvedení AIFO, pokud jde o fyzickou osobu nebo IČO, pokud jde o právnickou osobu. Pokud subjekt není řádně ztotožněn, pak získané údaje mohou být pouze informativní
- Záznamy (logy) o identifikaci žádajícího systému, času odpovědi, struktuře a obsahu poskytnutých údajů vede poskytující systém. Identifikaci poskytujícího systému, času přijetí odpovědi, struktuře a obsahu údajů vede přijímající systém. Referenční rozhraní zaznamenává identifikaci obou systémů, čas a strukturu předávaných údajů.
- Procesní provázání s eSSL v případě, kdy je referenční rozhraní využíváno k předávání dokumentů dle pravidel spisové služby. Toto se týká jen těch situací, kdy je obsahem skutečně dokument a nejedná se tedy jen o předávání dat.

ISSV bude využívat eGON služby dostupné prostřednictvím ISZR pro získání údajů ze:

- Registru obyvatel
- Registru osob
- Agendového informačního systému vyrozumívacího
- Převodník identifikátorů ORG (pro řešení výjimek zpracování AIFO)

A kompozitní služby ISZR pro získání údajů v případě, že požadované údaje nejsou v ZR vedeny z:

- Agendového informačního systému cizinců

ISSV bude dále využívat Informační systém sdílené služby (ISSS), který je základním rozhraním propojeného datového fondu veřejné správy. Tento informační systém je určen pro sdílení informací mezi jednotlivými agendovými informačními systémy. Integrace s ISSS bude využita pro komunikaci s:

- Portálem Občana pro předávání osvědčení o digitálním úkonu
- Kontaktním místem veřejné správy
- REZA

Pro autentizaci přistupujících uživatelů bude ISSV využívat

- Národní identitní autoritu (NIA) pro autentizaci veřejnosti
- Jednotný identitní prostor JIP/KAAS nebo Centrální autentizační a autorizační informační systém (CAAIS) pro autentizaci a autorizaci uživatelů informačního systému veřejné správy (ISVS), tedy ISSV

Některé úkony v rámci správy voleb vyžadují vedení spisu, protože nemohou být plně automatizovány. Proto bude nutné realizovat i integraci na spisovou službu. Integrace na spisovou službu bude realizována implementací standardu NSESSS pro komunikaci se systémy spisových služeb.

Některé z integrovaných systémů jsou dostupné přes internet. Centrální služby eGovernmentu jsou přístupné pouze prostřednictvím centrálního místa sdílených služeb CMS. Bude tedy nutné zajistit jak publikování příslušných rozhraní do veřejného internetu, tak i do CMS a zároveň zajistit přístup k definovaným systémům přes rozhraní (referenční rozhraní) v CMS.

3.4. DATOVÁ ARCHITEKTURA

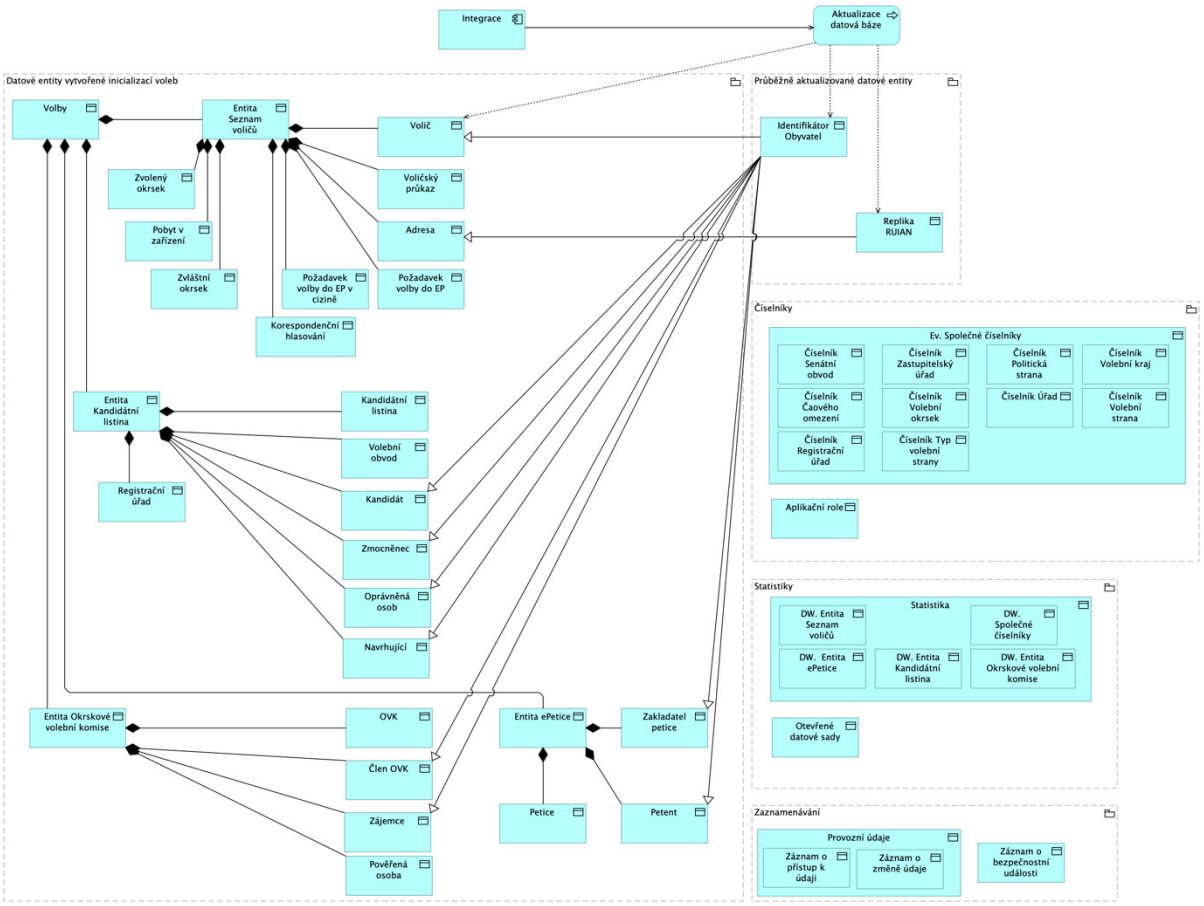
Systém obsahuje základní informace o voličích jako objekt „Identifikátor obyvatel“. Z tohoto objektu jsou děděna data do jednotlivých podskupin – volební seznam, zástupce, kandidát, člen volební komise

atd. Dalším základním datovým objektem je objekt „Volby“, který obsahuje základní informace ke každým jednotlivým volbám. Společně s objektem „Volební okrsek/volební obvod“ je možné řešit volební seznamy. Data jsou umístěna pouze jednou s jednotlivými vazbami, v systému neexistuje několik kopií dat pro jedny volby.

Principy organizace dat v systému budou následující:

- Bude existovat trvalý aktualizovaný datový kmen, který bude obsahovat:
  - Bázi subjektů založenou na evidenci AIFO – Identifikátor obyvatel, která bude průběžně aktualizována z ROB
  - Lokální evidenci územní identifikace (RUIAN) včetně historie, která bude průběžně aktualizována z RUIAN
  - Číselníky (volební okrsky a obvody, typy voleb, zastupitelské úřady, úřady, systémové činnosti)
  - Předpřipravené datové struktury určené pro inicializaci instancí evidencí entit Volby, Referendum, ePetice, Kandidátní listina, Volební komise
- Aktuální datové objekty vytvořené pro zajištění konkrétních procesů a výstupů v rámci organizace a správy voleb, například seznam voličů a kandidátní listiny
- Archiv aktuálních datových objektů uchovávaný omezenou dobu zabezpečených způsobem podle požadavků právních předpisů
- Datový sklad obsahující datové sady pro vytváření statistických pohledů a datové sady otevřených dat připravených k publikaci

Schéma datová architektura



Typ prvku	Jméno prvku	Popis prvku
Application process	Aktualizace datová báze	Aktualizace údajů již evidovaných subjektů. Probíhá použitím standardní eGON služby aisvCtiZmeny pro vyrozumívání o změně údajů a následným čtením údajů z ROB, CIS.
Data object	Identifikátor Obyvatel	Komponenta mimo systém ISSV. Představuje služby autentizace a případně autorizace reprezentované systém NIA a JIP/KAAS(CAAIS).
Data object	Replika RUIAN	Portál pro veřejnost zastřešuje část pro autentizovanou a část pro neautentizovanou veřejnost. Směrem k uživatelům je reprezentován webovým rozhraním pro veřejnost.
Data object	Seznam voličů a referenda (Veřejnost)	Realizuje aplikační logiku poskytující API funkce pro přístup k seznamu voličů a k referendům pro veřejnost.
Data object	Registr okrskových volebních komisí (Veřejnost)	Realizuje aplikační logiku poskytující API funkce pro přístup k registru okrskových volebních komisí pro veřejnost.
Data object	Nástroj ePetice (Veřejnost)	Realizuje aplikační logiku poskytující API funkce pro přístup k ePeticím pro veřejnost.
Data object	Registr kandidátních listin (Veřejnost)	Realizuje aplikační logiku poskytující API funkce pro přístup k registru kandidátních listin pro veřejnost.
Data object	Seznam voličů a referenda	Realizuje aplikační logiku poskytující API funkce pro přístup k seznamu voličů a k referendům pro interní uživatele.
Data object	Registr okrskových volebních komisí	Realizuje aplikační logiku poskytující API funkce pro přístup k registru okrskových volebních komisí pro interní uživatele.
Data object	Nástroj ePetice	Realizuje aplikační logiku poskytující API funkce pro přístup k ePeticím pro interní uživatele.
Data object	Registr kandidátních listin	Realizuje aplikační logiku poskytující API funkce pro přístup k registru kandidátních listin pro interní uživatele.
Data object	Statistika	Umožňuje definovat vlastní pohledy na předpřipravené datové sady. Tyto datové sady naplní datový sklad pomocí ETL nebo obdobného nástroje z dat jednotlivých registrů.
Data object	Modul správce ISSV	Aplikace pro správce umožní realizovat administraci a správu informačního systému v oblastech: • Správa entit • Archivace • Inicializace • Notifikace • Aktualizace dat • Správu plánovaných úloh

Typ prvku	Jméno prvku	Popis prvku
Data object	Potvrzení o digitálním úkonu	Komponenta realizující vytvoření a předání osvědčení o digitálním úkonu dle zákona č. 12/2020 Sb., o právu na digitální služby.
Data object	Integrace	Realizuje aplikační rozhraní k externím informačním systémům. Toto aplikační rozhraní konzumuje služby spisové služby, ISSS, ISRZ a poskytuje služby ISSS, využitelné i pro výdej dat a seznamů. Alternativní možnosti datového výdeje zmapuje přeimplementační analýza.
Data object	Spisová služba	Komponenta mimo systém ISSV. Poskytuje rozhraní NSESSS pro čtení i zápis dokumentů.
Data object	ISSS	Komponenta mimo systém ISSV. Informační systém sdílené služby dle zákona č. 111/2009 Sb., o základních registrech.
Data object	ISZR	Komponenta mimo systém ISSV. Informační systém základních registrů dle zákona č. 111/2009 Sb., o základních registrech.
Data object	ISDS	Komponenta mino systém ISSV. Informační systém datových schránek
Data object	REZA	Komponenta mino systém ISSV. Registr zastupování.
Data object	AIS ROB	Komponenta mimo systém ISSV. Základní registr obyvatel dle zákona č. 111/2009 Sb., o základních registrech.
Data object	AIS ROS	Komponenta mimo systém ISSV. Základní registr osob dle zákona č. 111/2009 Sb., o základních registrech.
Data object	RUIAN	Komponenta mimo systém ISSV. Základní registr územní identifikace, adres a nemovitostí dle zákona č. 111/2009 Sb., o základních registrech.
Data object	AIS CIS	Komponenta mimo systém ISSV. Informační systém cizinců podle zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky.
Data object	ORG	Komponenta mimo systém ISSV. Převodník identifikátorů zákona č. 111/2009 Sb., o základních registrech.
Data object	AISV	Komponenta mimo systém ISSV. Informační systém vyrozumívání dle zákona č. 111/2009 Sb., o základních registrech.
Data object	Entita seznam voličů	Zajišťuje perzistenci dat pro seznam voličů a referenda.
Data object	Entita Kandidátní listiny	Zajišťuje perzistenci dat pro registr kandidátních listin.
Data object	Entita ePetice	Zajišťuje perzistenci dat pro nástroj ePetice.
Data object	Entita Okrskové volební komise	Zajišťuje perzistenci dat pro registr okrskových volebních komisí.

Typ prvku	Jméno prvku	Popis prvku
Data object	Statistika	Datový sklad skládající se z datových sad pro vytváření datových pohledů a výstupů na základě definovatelných hledisek.
Data object	Společné číselníky	Zajišťuje perzistenci dat pro číselníky včetně jejich předchozích údajů.
Data object	Replika RUIAN	Lokální aktualizovaná kopie RUIAN obsahující historii údajů pro zajištění integrity dat v průběhu a po volbách.
Application service	Inicializace voleb	Reprezentuje aplikační službu, kterou zajistí ISSV.
Application service	Archivace voleb	Reprezentuje aplikační službu, kterou zajistí ISSV.
Application service	Inicializace, aktualizace a správa entit	Reprezentuje aplikační službu, kterou zajistí ISSV.
Application service	Provoz systému	Reprezentuje aplikační službu, kterou zajistí ISSV. Zajištění definovaných SLA na úrovni aplikační architektury, která zahrnuje aplikační a platformový software je v kompetenci Poskytovatele ISSV.
Application service	Nahlížení na údaje	Reprezentuje aplikační službu, kterou zajistí ISSV.
Application service	Provoz monitoringu	Reprezentuje aplikační službu, kterou zajistí ISSV. Monitoring stavu komponent aplikační architektury je nezbytný pro zajištění provozu a vyhodnocování SLA.
Application service	Bezpečnost	Reprezentuje aplikační službu, kterou ISSV umožní splnit definované požadavky na bezpečnost systému podle provedené analýzy rizik a v souladu s právními předpisy o kybernetické bezpečnosti. Dále IS implementuje zaznamenávání událostí tak, aby je bylo možné z jednoho místa v každém DC předávat k vyhodnocení na SIEM službu poskytovanou provozovatelem DC.
Application service	Notifikace	Reprezentuje aplikační službu, kterou zajišťuje ISSV.
Application service	Řízení změn	Reprezentuje aplikační službu, kterou architektura ISSV umožní realizovat. Aplikační komponenty musí pomocí dokumentace a řízení API, řízením a dokumentací verzí a dostupností repository balíčků a kontejnerů správně reagovat na požadavky ITIL procesů týkající se řízení změn a problémů v systému.

3.5. TECHNOLOGICKÁ ARCHITEKTURA

Objednatel a jeho Poskytovatel infrastruktury zajistí technologickou IT a komunikační architekturu formou služby poskytovanou státními datovými centry. Tato datová centra splňují požadavky pro provoz prvků kritické informační infrastruktury. Poskytované služby budou poskytovány jako cloud computing

služby v souladu s požadavky vyhlášky č. 316/2021 Sb., Vyhláška o některých požadavcích pro zápis do katalogu cloud computingu. Tyto služby je Poskytovatel infrastruktury schopen zabezpečit v rozsahu podmínek bezpečnostní úrovně nabízeného cloud computingu 3 – Vysoká s předpokladem budoucího zajištění bezpečnostní úrovně 4 - Kritická.

V rámci zajištění technologické IT a komunikační architektury budou poskytovány následující služby:

- Síťová konektivita (CMS2, případně internet)
- VPN přístup pro Poskytovatele aplikace
- Firewall
- Loadbalancing
- Advanced WAF
- VPN, site to site a uživatelská VPN
- Výpočetní výkon v podobě virtuálních serverů x86 (VMware, AzureStack) a IBM Power
- Diskové úložiště na diskových polích
- Zajištění provozu a podpory (včetně patchování) operačních systémů OS AIX, 7.3 a 7.2 Linux RHEL 9 a 8, Windows Server 2022 a 2019
- Hardening operačních systémů dle CIC Benchmarks
- Databázová platforma MS SQL, PostgreSQL 15.X, 14.X, 13.X a OracleDB
- Zálohování s využitím IBM Spectrum Protect
- Dohledové centrum zajistí provozní dohled IT v režimu 24x7
- Bezpečnostní dohled prostředí 24x7 SOC + Incident response zahrnuje bezpečnostní monitoring a log management
- Service Desk
- Testy (Disaster recovery, provozní)
- Mailové služby

Součástí služeb datových center je i spravovaná kontejnerizační platformy Red Hat OpenShift a Azure Kubernetes Service (AKS).

Uvedené služby budou poskytovány tak, jak jsou popsány v katalogu nabízených služeb. Katalog služeb SPCSS je veřejný dokument, dostupný na stránce https://www.dia.gov.cz/oha/katalog-cloud-computingu/nabidky-sluzeb-cloud-computingu-zapsanych-poskytovatelu/

pod odkazem:

https://www.dia.gov.cz/wp-content/uploads/2023/03/eGc-Nabidka_cloud_computingu-IaaS_PaaS_SaaS_c_1-2021_spol_Statni_pokladna_Centrum_sdilenych_sluzeb_-_20230119.pdf

Technologická architektura umožní:

- Provoz v hybridním režimu v on-premise virtualizovaném prostředí DC a ve virtualizovaném prostředí cloudů.
- Vysokou dostupnost aplikace provozované ve virtualizovaném prostředí v režimu active-passive v obou DC s online prováděnou datovou replikací a s možností transparentního přesunu dat a replikace mezi oběma DC v případě vzniku poruchy nebo havarijní situace. V případě služeb postavených nad platformou AzureStack je nutné vysokou dostupnost řešit na úrovni aplikace.

V rámci technologické architektury datových center budou vytvořena minimálně prostředí:

- Testovací
- Preprodukční

- Produkční

Požadované systémové zdroje budou definovány počtem stavebních bloků podle katalogu nabízených služeb.

Pro tato prostředí bude použito minimálně 5 serverů v každém DC (5 kubernetes nodů, nebo 3x aplikační + 2x DB servery) nebo adekvátní platformové služby AzureStack.

Aplikační architektura bude umožňovat při vysoké zátěži provoz v hybridním režimu, a to tím způsobem, že aplikační komponenty pro veřejnost budou provozovány v privátní části eGovernment cloudu.

Možnosti řešení vysoké dostupnosti na úrovni IaaS služeb DC jsou znázorněny na následujících schématech.

Schéma – virtuální server replikovaný active-passive

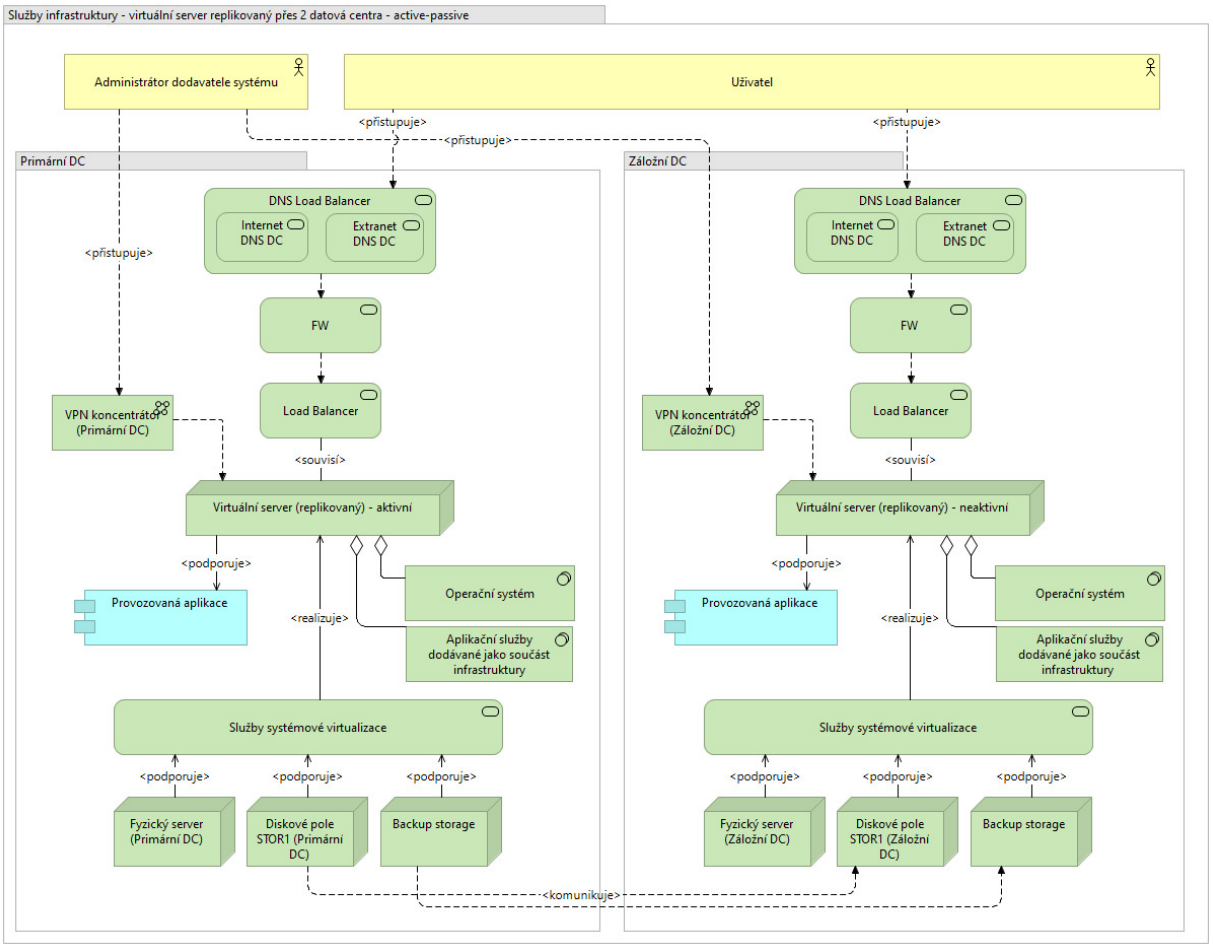
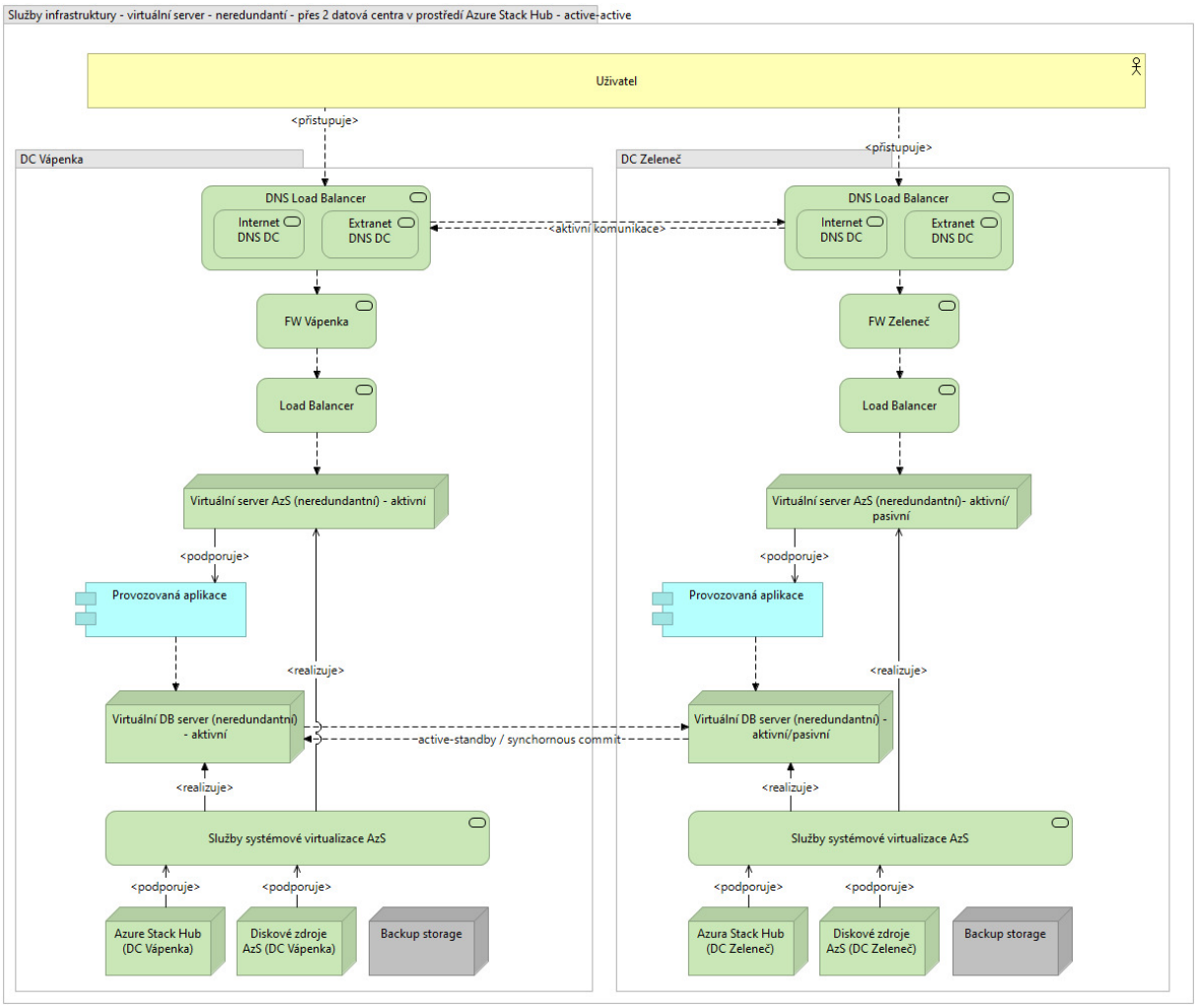


Schéma – virtuální server neredundantní active-active v AzureStack



Rozdělení působnosti a kompetencí v rámci Technologické a komunikační infrastruktury poskytovaných jako služba datových center.

Pro serverové komponenty platí předpoklad, že uživatelé na úrovni OS, DB nebo dalších poskytovaných služeb pro potřeby instalace, administrace nebo podpory provozu jsou vytvářeni, udržováni a spravováni Poskytovatelem infrastruktury a pomocí jeho nástrojů. Autentizace probíhá lokálně na úrovni serveru.

Oprávnění pro softwarové komponenty, které jsou součástí služeb Poskytovatele infrastruktury, jsou přidělována v souladu s požadavky instalovaných, resp. provozovaných aplikací, nicméně nejvyšší úroveň oprávnění (root, admin) nejsou přidělována mimo pracovníky Poskytovatele infrastruktury. V případě, že v rámci správy životního cyklu aplikace (instalace, upgrade) jsou tato oprávnění nezbytná pro provedení zásahu, jsou zajištěna prostřednictvím součinnosti Poskytovatele infrastruktury při zachování principu kontroly 4 očí.

Vzdálený přístup tzv. VPN je poskytován v rámci služeb DC Poskytovatele infrastruktury pro potřeby administrace, zpravidla pro potřeby Poskytovatele, a to jak pro fázi implementací, tak pro fázi provozní podpory. Přístupy jsou poskytovány na základě bezpečnostních přístupových profilů opravňujících přistoupit pouze ke službám, které jsou součástí služeb řešení.

Centrální služby správy uživatelů IS na úrovni administrace aplikace (IDM, LDAP nebo AD), pokud je Poskytovatel potřebuje jako součást navržené architektury, musí být součástí dodávky nabízeného IS.

Požadavky na správu uživatelů aplikace včetně jejich autentizace je součástí funkčních a technických požadavků poptávaného IS.

U všech SW komponent, používaných jako součást služeb, je dodržováno pravidlo průběžné aktualizace. V rámci služeb jsou provozovány aktuální uvolněná nebo maximálně jedna předchozí uvolněná verze (pro hlavní verzi – major release), případně aktuální nebo maximálně dvě předchozí uvolněné verze (pro vedlejší verzi – minor release).

Update či upgrade SW komponent, které jsou součástí služby, je prováděn jako součást řízení životního cyklu aplikací v rámci procesů podpory Poskytovatele infrastruktury a jsou součástí ceny služby. Poskytovatel infrastruktury stanovuje plán upgrade a update jím zpracovaných SW komponent, který projednává se Objednatelem a Poskytovatelem tak, aby plánované činnosti minimálně zasahovaly do využívání služeb a procesů podpory IS a služeb, nicméně stále platí výše uvedené pravidlo podporovaných verzí softwaru.

Poskytovatel se zavazuje, že při dodržování těchto pravidel, ať už během implementace nebo během podpory produktivního provozu, zajistí Poskytovali infrastruktury plnou součinnost ve všech částech řešení, za které je odpovědný.

Licence potřebné pro zajištění služby správy OS jsou její součástí. V případě virtualizační platformy VMWare je služba správy OS podporována výhradně pro OS Linux. V případě virtualizační platformy Azure Stack je služba správy OS podporována pro OS Windows i OS Linux.

Licence všech ostatních softwarových produktů, které nejsou součástí služby, musí být zajištěny jako součást dodávky IS.

Objednatel zároveň upozorňuje, že softwarové licence, které jsou součástí služeb, jsou ošetřené s ohledem na licenční podmínky příslušného výrobce. Pro softwarové licence, které Poskytovatel nabídne jako součást dodávky IS, musí být Poskytovatelem garantováno, že nebudou závislé na metrikách, jejichž splnění by omezovalo provozní a organizační procesy Poskytovatele infrastruktury (např. licence pro SW produkty, které jsou vázány na fyzické CPU).

Služba Provozní dohled poskytuje monitoring infrastruktury DC, sítí, HW, operačních systémů, databází a aplikací. Zajišťuje sběr událostí v jednotlivých vrstvách a částech systémů, které by mohly mít vliv na správný chod aplikací v případě výskytu definované odchylky od standardních požadovaných hodnot. Konfigurace odesílání logů ze zdrojů navrhovaného řešení do nástrojů provozního dohledu bude provedena Poskytovatelem v součinnosti s administrátory Poskytovatele infrastruktury a Objednatele. Náhled do provozního dohledu pro Poskytovatele není standardně poskytován.

Bezpečnostní monitoring pokrývá vybrané povinnosti definované zákonem č. 181/2014 Sb., o kybernetické bezpečnosti v platném znění, resp. vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti. Specifika dle klasifikace informací a povahy spravovaného systému (jako KII, VIS) jsou ze strany Objednatele určeny prováděcí smlouvou.
Jedná se o tyto opatření:

- § 14 Zvládání kybernetických bezpečnostních událostí a incidentů
- § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
- § 23 Detekce kybernetických bezpečnostních událostí
- § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí
- § 31 Kategorizace kybernetických bezpečnostních incidentů
- § 32 Forma a náležitosti hlášení kybernetických bezpečnostních incidentů

Součástí služby Bezpečnostní monitoring je rovněž:

- Vulnerability management (správa zranitelností) pro prověřování evidovaných aktiv na dostupné zranitelnosti.
- Pravidelný reporting o stavu služby, událostech a incidentech
- Přístup je poskytnut pouze určeným pracovníkům Objednatele do prostředí SIEM, kde mohou sledovat aktivity, které generují monitorované systémy.

Konfigurace odesílání logů ze zdrojů navrhovaného řešení do SIEM bude provedena Poskytovatelem v součinnosti s administrátory Poskytovatele infrastruktury. Pro zajištění korektní interpretace je Poskytovatel povinen dodat popis aplikačních logů a postup pro incident response.

4. POŽADAVKY NA FUNKCIONALITY

4.1. MODUL SEZNAM VOLIČŮ

4.1.1. ÚVOD

Cíle:

- vytvoření jednotného seznamu voličů nahrazujícího dosavadní stálé, zvláštní a dodatkové seznamy
- zrušení místní příslušnosti pro některé úkony, např. pro vydání voličského průkazu
- umožnění přístupu voliče ke svým datům
- umožnění elektronizace úkonů občana ve vztahu k účasti ve volbách, ne však vlastního provedení volby
- snížení chybovosti a snížení administrativní zátěže

Obsah

- Údaje o voličích pro volby do zastupitelstev územních samosprávných celků, Parlamentu České republiky, Evropského parlamentu, volbu prezidenta a referenda.
- Provozní data monitorující činnost systému a přístup k osobním údajům.

4.1.2. DATA

Údaje vedené v seznamu voličů jsou stanoveny v § 23 odst. 1 až 3, jejich zpřístupňování je stanoveno v § 24 odst. 1 a 2 [NZSV].

Údaje o voliči vedené podle § 23 odst. 1 NZSV (datum narození, státní občanství, adresa a druh pobytu) se ze systému odstraňují poté, co dojde k úmrtí subjektu údajů nebo, jde-li o cizince, k ukončení pobytu.

Údaje o voliči vedené podle § 23 odst. 2 NZSV (jméno, příjmení a další údaje specifické pro konkrétní volby) se v informačním systému uchovávají po dobu 90 dnů ode dne vyhlášení výsledků voleb.

Tabulka 1 – Přehled entit

název entity	**Popis**
Adresa	Podmnožina RUIAN obsahující údaje potřebné správu voleb.
Číselník Senátní obvod	Číselník senátních volebních obvodů.
Číselník Úřad	Číselník městských úřadů, městských částí nebo obvodů a dalších úřadů podílejících se na organizaci voleb.
Číselník Volební kraj	Číselník volebních krajů.
Číselník Zastupitelský úřad	Číselník zastupitelských úřadů České republiky.
Korespondenční hlasování	Záznam o vydání písemností ke korespondenčnímu hlasování.
Pobyt v zařízení	Oznámení správce zařízení o pobytu voliče na adrese zařízení.
Požadavek volby do EP	Oznámení cizince o volbě do Evropského parlamentu na území České republiky.
Replika RUIAN	Pravidelně aktualizovaná kopie RUIAN obsahující historii.
Volby	Atributy voleb.
Volby do EP v cizině	Oznámení o volbě do Evropského parlamentu mimo území České republiky.
Identifikátor obyvatel	Identifikační údaje voliče nebo osoby, která se má stát voličem v rozsahu § 23 odst. 1 NZSV
Volič	Osobní údaje a další atributy voliče potřebné správu voleb.
Voličský průkaz	Záznam o vydání voličského průkazu opravňujícího k volbě v jiném volebním okrsku než domovském.

název entity	Popis
Zvláštní okrsek	Záznam o změně domovského volebního okrsku na volební okrsek vedený při zastupitelském úřadě ČR.
Zvolený okrsek	Záznam o změně domovského volebního okrsku na volební okrsek zvolený voličem.

4.1.3. ČINNOSTI

Iniciální naplnění datové báze

Při plnění datové báze jsou kvůli bezpečnosti dat vyloučeny přenosy dat na paměťových médiích a jsou použity výhradně standardní služby základních registrů.

Iniciální naplnění údajů entity Identifikátor obyvatel, tzn. identifikačních údajů voličů a osob, které se mají stát voliči, proběhne z registru obyvatel získáním AIFO relevantních fyzických osob prostřednictvím eGON služby iszrPodejMapaAifo a následným čtením údajů data narození, státní příslušnosti a adresy pobytu těchto osob standardní službou robCtiHromadneAifo2, případně aiscCtiAifo2 pro získání druhu pobytu cizinců.

Iniciální naplnění entity Replika RUIAN proběhne daty ze souborů VFR (výměnného formátu RUIAN), jejichž adresy jsou předány službou ruianSouboryDat.

Aktualizace datové báze

Aktualizace údajů již evidovaných subjektů entity Identifikátor obyvatel probíhá použitím standardní eGON služby aisvCtiZmeny pro vyrozumívání o změně údajů a následným čtením údajů z ROB službou robCtiHromadneAifo2 s vynecháním zrušených záznamů subjektů, jejichž AIFO je obsaženo ve výstupu orgCtiZmenyAIFO. Pro cizince se službou aisvCtiZmeny zjišťuje případná změna druhu pobytu, která se následně načte službou aiscCtiAifo2.

Během aktualizace je nezbytné řešit změny AIFO vzniklé v důsledku slučování nebo rozdělování identit v editorských systémech. Záznamy, jejichž identifikátor je obsažen ve výstupu orgCtiZmenyAIFO jsou zrušeny.

Aktualizace entity Identifikátor obyvatel doplněním o údaje subjektů nově zařazených do ROB probíhá použitím standardní eGON služby aisvCtiZmenyZaloz pro vyrozumívání o změně údajů a následným čtením údajů z ROB službou robCtiHromadneAifo2, případně aiscCtiAifo2 pro získání druhu pobytu cizinců.

Pokud je entita Volič pro konkrétní volby v aktualizovatelném stavu, tzn. v časovém intervalu ohraničeným vyhlášením voleb a zahájením generování seznamů voličů, probíhá i aktualizace jejích údajů.

Aktualizace Repliky RUIAN probíhá s použitím eGON služby ruianCtiSeznamZmen, která získá informace o změnách prvků územní identifikace. Aktualizace bude probíhat v intervalech 30 minut, aby se zajistila aktuálnost dat územní identifikace potřebná pro on-line činnosti. Na data jednotlivých změněných prvků se dotazuje pomocí eGON služeb E35a až E35t.

Tabulka 2 – Činnosti – Systém

	proces
SY01	uzavření seznamu voličů

Tabulka 3 – Činnosti – Obec

	proces
OB01	zápis do volebního okrsku na základě pobytu v zařízení
OB02	zrušení zápisu do volebního okrsku na základě pobytu v zařízení
OB03	zápis do jiného volebního okrsku
OB04	zrušení zápisu do jiného volebního okrsku
OB05	zrušení zápisu pro volbu u zastupitelského úřadu
OB06	zápis cizince pro volby do EP
OB07	zrušení zápisu cizince pro volby do EP
OB08	vydání voličského průkazu
OB09	ověření (vyhledání) vydání voličského průkazu
OB10	ověření zápisu voliče na jeho žádost
OB11	sestavení rozdělovníku pro distribuci volebních tiskovin voličům
OB12	stažení výpisů ze seznamu voličů
OB13	vytvoření pomocného výpisu ze seznamu voličů pro zařízení
OB14	statistiky
OB15	zápis referenda
OB17	kontroly
OB18	vytvoření seznamu hlasujících pro místní referendum

Tabulka 4 – Činnosti – Krajský úřad

	proces
KR01	zápis referenda

Tabulka 5 – Činnosti – Zastupitelský úřad

	proces
ZU01	zápis pro volbu u zastupitelského úřadu
ZU02	zrušení zápisu pro volbu u zastupitelského úřadu
ZU03	vydání voličského průkazu
ZU04	vydání písemností pro korespondenční hlasování
ZU05	stažení výpisů ze seznamu voličů
ZU06	zápis do jiného volebního okrsku
ZU07	zrušení zápisu do jiného volebního okrsku

Tabulka 6 – Činnosti – Ministerstvo vnitra

	proces
MV00	zápis voleb
MV01	zápis údaje o zapsání českého občana pro volby do EP v cizině
MV02	nahlížení do seznamu voličů

	proces
MV03	pokyn k uzavření seznamu pro volby konané na celém území a pro volby do Senátu
MV04	Pověření POU k zastupování OU
MV05	Zrušení pověření POU k zastupování OU

Tabulka 7 – Činnosti – Volič

	proces
VO01	zápis do jiného volebního okrsku
VO02	zrušení zápisu do jiného volebního okrsku
VO03	zápis cizince pro volby do EP
VO04	zrušení zápisu cizince pro volby do EP
VO05	vydání voličského průkazu
VO06	ověření zápisu voliče
VO07	žádost o korespondenční hlasování

4.2. MODUL REGISTR KANDIDÁTNÍCH LISTIN

4.2.1. ÚVOD

Cíle:

- vytvoření, podání, kontrola a registrace kandidátních listin,
- příprava podkladů pro výrobu hlasovacích lístků,
- dálkový přístup volební strany k nástrojům pro vytvoření kandidátní listiny,
- dálkový přístup veřejnosti k přehledu volebních stran a náhledům hlasovacích lístků.

Obsah:

- obecné údaje o podmínkách registračního řízení,
- údaje z elektronických formulářů uložených v informačním systému volebními stranami,
- údaje z podaných kandidátních listin uvedené včetně osobních údajů kandidátů a zvláštních náležitostí stanovených zákonem o volbách,
- údaje o průběhu a výsledku registračního řízení a obsah registrovaných kandidátních listin,
- údaje o historii přístupů a změn v obsahu registru kandidátních listin,
- datové úložiště s elektronickými obrazy dokumentů registračního řízení,
- výstupy pro přípravu a výrobu hlasovacích lístků a náhledy hlasovacích lístků.

Údaje vedené v registru kandidátních listin jsou stanoveny v § 25 odst. 1, přístup do registru je stanoven v § 25 odst. 2 až 5, skartační lhůta je stanovena v odst. 6 [NZSV].

4.2.2. DATA

Tabulka 8 – Přehled entit

název entity	**popis**
Volby	atributy voleb (totožná s entitou volby uvedenou v Seznamu voličů)
Volební obvod	atributy volebního obvodu
Registrační úřad	úřad vedoucí registrační řízení
Číselník Registrační úřad	číselník registračních úřadů

název entity	popis
Podmínky registrace	podmínky registračního řízení
Kandidátní listina	atributy pro vytvoření a ověření kandidátní listiny a vytvoření výstupů pro výrobu hlasovacích lístků.
Kandidát	atributy pro identifikaci kandidáta, údaje o politické příslušnosti, navrhující straně, pořadí na kandidátní listině
Zmocněnec	atributy pro identifikaci zmocněnce nebo jeho náhradníka, kontaktní údaje
Oprávněná osoba	atributy pro identifikaci osoby oprávněné jednat jménem volební strany, její kontaktní údaje
Navrhující	atributy pro identifikaci navrhujícího subjektu, datum zpřístupnění petice k podepisování
Číselník Politická strana	rejstřík politických stran a politických hnutí vedený s omezenou položkovou skladbou
Číselník Volební strana	číselník volebních stran navazující na číselník ČSÚ
Změny kandidátní listiny	změny údajů a stavů kandidátních listin

4.2.3. ČINNOSTI

Tabulka 9 – Činnosti – Zmocněnec

	proces
ZM01	založení účtu zmocněnce
ZM02	podání kandidátní listiny
ZM03	autorizace kandidátní listiny
ZM04	zobrazení stavu podání kandidátní listiny

Tabulka 10 – Činnosti – Registrační úřad

	proces
RU00	Zveřejnění podmínek registračního řízení
RU01	Úprava volebních obvodů
RU02	Zobrazení seznamu podání kandidátních listin
RU03	Kontrola shody podané a autorizované verze kandidátní listiny
RU04	Kontrola údajů kandidátní listiny
RU05	Kontrola duplicit
RU06	Kontrola petic
RU07	Registrace kandidátní listiny
RU08	Losování čísel volebních stran
RU09	Odvolání/vzdání se kandidáta
RU10	Odvolání zmocněnce
RU11	Ustanovení nového zmocněnce
RU12	Schválení kandidátní listiny pro tisk hlasovacích lístků
RU13	Uvolnění kandidátních listin pro tisk hlasovacích lístků
RU14	Schválení tiskové podoby hlasovacích lístků
RU21	Zpřístupnění pro ČSÚ

Tabulka 11 – Činnosti – Systém

	proces
SY00	Inicializace
SY01	Zpřístupnění pro ČSÚ

Tabulka 12 – Činnosti – Ministerstvo vnitra

	proces
MV00	Zápis voleb
MV01	Nahlížení do kandidátních listin
MV02	Nahlížení do úložiště dokumentů
MV03	Nahlížení do úložiště hlasovacích lístků
MV04	Správa číselníků

Tabulka 13 – Činnosti – Český statistický úřad

	proces
SU01	Převzetí dat

Tabulka 14 – Činnosti – ÚDHPSPH

	proces
UD01	Náhled na kandidátní listinu

Tabulka 15 – Činnosti – výrobce hlasovacích lístků

	proces
VL01	Převzetí dat pro výrobu hlasovacích lístků
VL02	Předání hlasovacích lístků ke korekturám

Tabulka 16 – Činnosti – Veřejnost

	proces
VE01	Přehled volebních stran
VE02	Zobrazení hlasovacích lístků
VE03	Zobrazení kandidátních listin

4.3. MODUL REGISTR ČLENŮ OKRSKOVÝCH VOLEBNÍCH KOMISÍ

4.3.1. ÚVOD

Hlavním cílem registru členů okrskových volebních komisí je

- usnadnění komunikace kandidujících subjektů s obcemi při delegování členů okrskových volebních komisí a

- poskytnutí nástroje pro ustanovení okrskových volebních komisí.

Údaje vedené v registru okrskových volebních komisí jsou stanoveny v § 26 odst. 1 a 2, jejich zpřístupňování je stanoveno v § 26 odst. 3 až 5 [NZSV].

Údaje o členech okrskových volebních komisí se v informačním systému uchovávají po dobu 90 dnů ode dne ukončení činnosti všech okrskových volebních komisí v příslušných volbách.

4.3.2. DATA

Tabulka 17 – Přehled entit

název entity	**Popis**
OVK	okrsková volební komise
Člen OVK	člen OVK (delegovaný a jmenovaný člen a člen, který složil slib) a náhradník
Zájemce	zájemce o výkon činnosti člena komise z široké veřejnosti
Pověřená osoba	osoba pověřená zmocněncem (nezávislým kandidátem, navrhujícím občanem) delegováním členů OVK

4.3.3. ČINNOSTI

Tabulka 18 – Činnosti – Systém

	proces
SY01	Založení seznamu OVK

Tabulka 19 – Činnosti – Ministerstvo vnitra

	proces
MV01	Přidělení přístupu politickým stranám v prezidentských volbách
MV02	Výstup agregovaných údajů
MV03	Přístup k údajům

Tabulka 20 – Činnosti – Zmocněnec

	proces
ZM01	Určení pověřené osoby
ZM02	Delegování členů OVK
ZM03	Vytvoření profilu pověřené osoby

Tabulka 21 – Činnosti – Pověřená osoba

	proces
PO01	Delegování členů OVK

Tabulka 22 – Činnosti – Zájemce

	proces
ZA01	Přihlášení zájemce
ZA02	Editování údajů zájemce
ZA03	Zrušení záznamu zájemce

Tabulka 23 – Činnosti – Obec

	proces
OB01	Naplnění seznamu OVK
OB02	Ověření delegovaných osob
OB03	Kontrola duplicit
OB04	Rozdělení do OVK
OB05	Automatické rozdělení do OVK
OB06	Jmenování členů OVK starostou
OB07	Rozesílání pozvánek
OB08	Zobrazení a editace OVK
OB09	Modul odměn
OB11	Přihlášení zájemce
OB12	Editování údajů zájemce
OB13	Zrušení záznamu zájemce

Tabulka 24 – Činnosti – Veřejnost

	proces
VE01	Přístup k veřejným údajům OVK

4.4. MODUL PRO SESTAVOVÁNÍ ELEKTRONICKÝCH PETIC

4.4.1. ÚVOD

Nástroj pro sestavování elektronických petic, dále jen ePetice, slouží volebním subjektům, jejichž kandidatura vyžaduje podle zákona podporu voličů formou petice:

1) Umožňuje online zakládání a podporu elektronických petic s využitím zaručené elektronické identity.
2) Elektronickou petici lze založit pouze pro nejbližší volby.
3) Kandidát uděluje souhlas se založením petice na svoji podporu (ověřený podpis), nelze založit petici bez souhlasu kandidáta, to neplatí pro sdružení nezávislých kandidátů.
4) Kandidát má právo zrušit petici na svoji podporu.
5) Pro jedny volby nelze založit více petic, petice obsahuje jedinečný osobní identifikátor kandidáta nebo jedinečný název volební strany skupiny nezávislých kandidátů.

Údaje obsažené v elektronickém výstupu z petice jsou stanovené příslušným zákonem o volbách.

Údaje v nástroji pro sestavování elektronických petic se uchovávají po dobu 10 kalendářních let následujících po kalendářním roce, v němž bylo příslušné registrační řízení ukončeno.

4.4.2. DATA

Tabulka 25 – Přehled entit

název entity	**Popis**
Petice	Identifikace petice
Zakladatel petice	Subjekt zakládající petici
Petent	Volič podporující kandidáta

4.4.3. ČINNOSTI

Tabulka 26 – Činnosti – Kontaktní místo veřejné správy

	proces
KM01	Založení petice
KM02	Změna zakladatele petice

Tabulka 27 – Činnosti – Zakladatel petice

	proces
ZP01	Nahlížení do petice
ZP02	Uzavření petice
ZP03	Uložení obsahu petice
ZP04	Předání petice
ZP05	Přihlášení petice k volbám

Tabulka 28 – Činnosti – Ministerstvo vnitra

	proces
MV01	Zrušení petice

Tabulka 29 – Činnosti – Systém

	proces
SY01	Otevření petice
SY02	Uzavření petice
SY03	Skartace petice
SY04	Zápis termínu voleb

Tabulka 30 – Činnosti – Registrační úřad

	proces
RU01	Nahlížení do petice
RU02	Stažení petice

Tabulka 31 – Činnosti – Petent

	proces
PE01	Podpis petice a ověření, zda uživatel již petici podepsal

Tabulka 32 – Činnosti – Veřejnost

	proces
VE01	Přístup k veřejným údajů ePetice

4.5. FUNKCIONALITA FORMULÁŘE

Funkcionalita elektronické formuláře bude obsahovat nástroj pro správu formulářů, samotné vytváření formulářů a provázání na databázi ISSV a integrované systémy bude řešeno dodavatelsky.

Formuláře budou k dispozici v části ISSV vázané na důvěryhodnou autentizaci.

V rámci polí formuláře bude možné navázat tyto atributy na existující dostupné atributy za pomoci integrace na PPDF a základní registry. Tyto atributy budou vyplňovány v rámci prohlížeče automaticky z daného datového zdroje.

U kolonek bude možné nastavit jejich masku v rámci vytvoření a editace kolonky. Masky budou obsahovat předdefinované masky (např. telefon, e-mail, jméno, adresa, PSČ apod.) a v případě, že v rámci prohlížeče bude následně uživatel vkládat údaje ve špatném formátu, bude na to upozorněn a vyzván k jejich opravě, nebude možné formulář s těmito špatně vloženými údaji odeslat.

U kolonek bude možné stanovit, zda se jedná o povinně vyplňované kolonky nebo volitelně vyplňované. U povinně vyplňovaných pak nebude v rámci prohlížeče možné odeslat formulář bez jejich vyplnění. Formuláře umožní vkládání loga a jiných grafických či HTML prvků.

Formulář by měl umožnit podpis formuláře přes elektronický podpis – minimálně s využitím důvěryhodného ověření uživatele při autentizaci, konkrétní detail bude řešit předimplementační analýza. Tento požadavek (podpis formuláře) bude zadáván v rámci vytvoření formuláře.

Odeslané formuláře budou vytěžovány do databáze ISSV a rovněž budou zaslány do eSSL.

Vytvoření a publikaci formulářů do ISSV bude zajišťovat Poskytovatel.

Z pohledu uživatele by mohlo vyplnění vypadat následovně:

Uživateli bude po autentizaci a vybrání formuláře k vyplnění zobrazen daný elektronický formulář, který následně vloží po odsouhlasení uživatele automaticky doplňované údaje z dostupných zdrojů. Pokud nebudou tyto údaje k dispozici, bude možné je vyplnit uživatelsky, avšak tyto atributy budou obsahovat v metadatech informaci, že se jedná o uživatelem vkládané údaje.

Při vyplňování bude uživatel upozorňován na špatně zadávané údaje za pomocí masek kolonek formuláře. Po vyplnění formuláře před jeho odesláním dojde k automatické kontrole a v případě, že nebudou vyplněny povinné údaje a/nebo budou kolonky vyplněny ve špatném formátu, bude vyzván uživatel k nápravě s vyznačením chyb a upozorněním na chyby. Součástí podávaného formuláře mohou

být přílohy. K formuláři tedy bude možné přiložit přílohy, přičemž pole pro přílohu rovněž půjde vyznačit jako povinné, stejně jako kolonky formuláře.

Při vyplňování formuláře bude možné si formulář uložit v rozpracovaném stavu a později se k němu vrátit, pokud bude v té době formulář stále platný nebo nebude stanoveno časové omezení k návratu do formuláře.

Před odesláním může být uživatel vyzván k podpisu, bude-li to formulář vyžadovat.

Formulář bude následně odeslán ISSV s využitím ISDS do spisové služby a rovněž dojde k vytěžení atributu formuláře do DB ISSV.

Konkrétní výčet cílových formulářů a namapováni atributů na DB bude řešit předimplementační analýza.

V rámci dodání Díla je vyžadováno po Poskytovateli navržení, dodání a implementace 25 formulářů do ISSV a jeho funkcionalit vč. provázání atributů formulářů na data základních registrů s předvyplněním údajů, vytvoření kontrolních masek polí formuláře a provázání polí formulářů na DB ISSV. Vyžadované formuláře jsou uvedeny níže:

Modul seznamu voličů

- Žádost o voličský průkaz
- Žádost o hlasování v jiném okrsku
- Žádost o hlasování ve zvláštním volebním okrsku
- Žádost o vyškrtnutí ze zvláštního volebního okrsku
- Žádost o hlasování ve volbách do EP v ČR
- Žádost o zrušení nahlášení k hlasování ve volbách do EP v ČR
- Žádost o ověření údajů, které jsou o voliči vedeny v seznamu voličů
- Žádost o korespondenční hlasování

Modul registru kandidátních listin

- Vytvoření uživatelského profilu zmocněnce
- Podání kandidátní listiny
- Doplnění kandidátní listiny
- Zpětvzetí kandidátní listiny
- Odvolání kandidatury
- Vzdání se kandidatury
- Nahlížení do „spisu“
- Stahování údajů z kandidátek pro účely tvorby hlasovacích lístků

Modul registru okrskových volebních komisí

- Delegace členů/náhradníků do okrskových volebních komisí v obci
- Pověření k delegaci jinou osobou než zmocněncem
- Odvolání člena okrskové volební komise
- Vzdání se členství v okrskové volební komisi
- Nahlášení do „zásobníku“ zájemců o členství v okrskové volební komisi

Modul nástroje pro sestavování elektronických petic

- Založení ePetice na podporu kandidatury
- Podpis (prohlášení o podpoře) ePetice
- Pořízení výpisu z elektronické petice
- Souhlas/odvolání souhlasu kandidáta se založením petice

Další formuláře budou Poskytovatelem dodány v rámci služeb na objednávku.

4.6. FUNKCIONALITA STATISTIKA

V rámci statistiky bude řešeno vytváření datových sad otevřených dat. V rámci otevřených dat budou dostupné údaje o registračním řízení, podaných kandidátních listinách (k rozsahu údajů srov. DPIA) a zaregistrovaných kandidátech. Dále zde budou informace o způsobu hlasování, včetně překladů do českého znakového jazyka a včetně verzí pro snadné čtení. Systém poskytne i adresář volebních místností a seznam kandidátů na volby.cz.

Pro vytváření datových sad bude využit nástroj ETL, který bude číst data z evidenčních databází.

Statistika bude disponovat vlastním rozhraním.

4.7. FUNKCIONALITA ADMINISTRACE

Funkcionalita pro správce umožní realizovat administraci a správu informačního systému v oblastech:

- Správa entit
- Archivace
- Inicializace
- Notifikace
- Aktualizace dat
- Správu plánovaných úloh

Administrace bude disponovat vlastním zabezpečeným rozhraním.

5. SYSTÉMOVÉ POŽADAVKY ISSV

5.1. INTEGRACE

ISSV bude disponovat integrační platformou, umožňující napojení systému na další informační systémy a aplikace.

Pro komunikaci s agendovými informačními systémy veřejné správy bude ISSV využívat Referenční rozhraní v souladu s jeho definicí zakotvenou zejména v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů a zákoně č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. Využívání údajů prostřednictvím referenčního rozhraní je vždy realizováno výhradně na základě příslušných oprávnění evidovaných v registru práv a povinností (RPP) definovaných při ohlášení Agendy v AIS Působnostním.

Budou realizovány minimálně následující integrace:

- Integrace na NIA
- Integrace na JIP/KAAS
- Integrace na CAAIS
- Integrace na eSSL Objednatele
- Integrace na ISDS
- Integrace na ROB
- Integrace na ROS
- Integrace na RÚIAN
- Integrace na eGSB
- Integrace na REZA
- Integrace na AISV
- Integrace na ORG
- Integrace na CIS
- Integrace na AISEO
- Integrace na IDM Objednatele (na bázi Microsoft Active Directory)

Objednatel zajistí Poskytovateli nezbytnou součinnost správce či Poskytovatele IS, s nímž bude ISSV integrován.

Větší detail integrací je uveden v kapitole Aplikační architektura – integrace.

Předmětem předimplementační analýzy bude kromě analýzy požadovaných integrací výše řešeno **napojení Díla na Dohledové centrum eGovernmentu** (DCeGOV), přičemž součástí analýzy bude služba zajišťující automatizované předávání logů na monitoring DCeGOV a služba pro automatizované předávání událostí ze Service Desk ISSV na Service Desk DCeGOV pro relevantní události. Následná realizace integrace na DCeGOV a služeb bude v rámci dodání Díla řešena v případě rozhodnutí Objednatele o realizaci integrace na bázi služeb na objednávku dle čl. 5.1 smlouvy. Detail požadavku na analýzu i realizaci je uveden v příloze č.1 tohoto dokumentu. Objednatel si současně vyhrazuje možnost změny rozsahu předimplementační analýzy spočívající v neprovedení analýzy napojení Díla

na DCeGOV, a to na základě písemného požadavku Objednatele. Tato redukce rozsahu předimplementační analýzy bude řešena postupem dle smlouvy.

Objednatel si dále vyhrazuje požadovat provedení analýzy napojení (integrace) Díla na alternativní dohledové centrum odlišné od DCeGOV a následnou realizaci integrace Díla na takové alternativní dohledové centrum, a to na základě služeb na objednávku dle čl. 5.1 smlouvy.

5.2. AUTENTIZACE A AUTORIZACE

5.2.1. UŽIVATELSKÝ PROFIL

Systém umožňuje vytvoření profilu autentizovaného uživatele jako pověřené osoby. Vytvoření profilu je v kompetenci Zástupce, viz Registr členů OVK.

Takto vytvořené uživatelské profily obsahují údaje uvedené v kapitole Entita Pověřená osoba, údaje jsou uloženy v lokální databázi uživatelů v modulu správa uživatelských přístupů. V případě autentizace uživatele k danému modulu, je nejdříve ověřeno jeho stanovení do role pověřené osoby. Pokud není již role nastavena je ověřen uživatel vůči záznamům stanovených pověřených osob zda-li může uživatel vykonávat danou roli a v případě kladného výsledku ověření, je mu tato tole přidělena po dobu platnosti daného uživatelského profilu.

5.2.2. IDENTIFIKACE A AUTENTIZACE UŽIVATELŮ – VOLIČŮ A PETENTŮ, ZMOCNĚNCŮ

V souladu se zákonem č. 250/2017 Sb. o elektronické identifikaci, je identifikace (ztotožnění) a autentizace (proces ověření identity) uživatelů (neanonymní uživatel) prováděna prostřednictvím kvalifikovaného systému elektronické identifikace. Národní bod (dále také NIA) je informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému.

Minimální požadovaná úroveň záruky pro elektronickou identifikaci je pro ISSV stanovena jako značná.

NIA poskytne (po úspěšně provedené autentizaci uživatele) ISSV prostřednictvím systému základních registrů AIFO uživatele, pokud je úspěšné ztotožnění s ROB, a BSI identifikátor eIDAS.

5.2.3. IDENTIFIKACE A AUTENTIZACE UŽIVATELŮ – VOLEBNÍCH ORGÁNŮ

Pro autentizaci uživatelů – volebních orgánů systém využívá autentizační webové služby KAAS. ISSV provede přesměrování neautentizovaného uživatele na přihlašovací stránku KAAS. Po úspěšném ověření uživatele získá ISSV autentizační token uživatele.

Komponenta Správa uživatelů ISSV zavolá autentizační webovou službu KAAS za účelem získání informací o uživateli. Webové službě předá autentizační token uživatele. Pokud je token platný, ISSV v odpovědi obdrží informace o uživateli:

- uživatelské jméno,
- jméno a příjmení,
- zkratka subjektu, v němž má uživatel zřízen přístup,
- seznam aplikačních přístupových rolí přidělených uživateli,
- seznam agendových činnostních rolí přidělených uživateli.

Aplikační přístupové role se týkají AIS a určují, jakou roli má uživatel v AIS. Tyto role definuje garant AIS. Agendové činnostní role se týkají základních registrů a určují, k jakým referenčním údajům v ZR může uživatel přistupovat. Agendové činnostní role ISSV nevyužívá.

Aby mohl systém aplikační přístupové role z JIP/KAAS využívat, správce ISSV definuje aplikační přístupové role ISSV v JIP.

5.2.4. AUTORIZACE A SPRÁVA UŽIVATELSKÝCH PŘÍSTUPŮ

Správa uživatelských přístupů je komponenta ISSV, jejímž cílem je správa a přiřazování aplikačních rolí autentizovaným uživatelům a správa uživatelských účtů systému. Autentizační komponenta dále zprostředkovává přihlášení oprávněných uživatelů s využitím služeb NIA a JIP/KAAS. Tato komponenta také uchovává údaje uživatelů pro účely dohledávání uživatelských identifikátorů v auditním logu.

Správa uživatelů poskytuje tyto funkce:

- Správa identit a jejich profilů
- Správa aplikačních rolí systému
- Propojování informací o jednoznačné identitě (NIA) s údaji v profilu uživatele. Tato funkčnost se týká zmocněnců, zástupců zmocněnců.
- Autorizace uživatele k funkcím systému založené na přiřazení aplikační role uživateli nebo aplikační přístupové roli. Tato funkčnost se týká uživatelů – volebních orgánů autentizovaných službou KAAS.

Komponenta Správa uživatelských účtů uchovává spravované informace v databázi uživatelských účtů. Dále také uchovává údaje uživatelů pro účely dohledávání uživatelských identifikátorů v auditním logu.

Uživatel – volič je po autentizaci autorizován v roli volič, profil se nevytváří a realizovaný přístup do systému se na profil nemapuje. Přístup je zaznamenán do logu.

5.3. MIGRACE DAT

Migrace dat se nepředpokládá. Úvodní naplnění datového kmene systému bude provedeno s využitím eGON služeb systému základních registrů.

Naplnění je popsáno v kapitole Požadavky na funkcionality.

5.4. IMPLEMENTACE

ISSV bude nejprve vyvíjen v rámci vývojového prostředí Poskytovatele. Implementace následně proběhne ve dvou fázích. První fází bude implementace ISSV do testovacího prostředí, vytvořeného na cílové infrastruktuře a druhou fází bude implementace ISSV do produkčního prostředí.

Pro implementaci je nezbytné stanovit požadavky na nosné prostředí a jeho konfiguraci, požadavky se budou odvíjet od předimplementační analýzy a performance testů ISSV ve vývojovém prostředí, obojí bude zajištěno Poskytovatelem. Požadavky na implementaci budou diskutovány s Poskytovatelem infrastruktury Objednatele.

Implementace bude realizovaná jako řízená a bude koordinovaná s Objednatelem a technickými správci Objednatele.

5.5. ŽIVOTNÍ CYKLUS

Životní cyklus ISSV bude následující:

Realizace IS

Vývojová část:

(1) Analýza a vytvoření analytické dokumentace
(2) Vývoj ISSV
(3) Vývojové testování
(4) Příprava k migraci

Implementace:

(1) Implementace do cílového prostředí Objednatele
(2) Konfigurace systému v cílovém prostředí
(3) Realizace integrací ISSV v cílovém prostředí
(4) Testování v cílovém prostředí, bezpečnostní testy
(5) Odstranění nedostatků

Uvedení do provozu:

(1) Předání dokumentace, práv a zdrojových kódů
(2) Zaškolení uživatelů, předání školící dokumentace
(3) Řízení zpřístupnění ISSV
(4) Asistence při pilotním provozu

Rozvoj ISSV nad rámec původních požadavků:

(1) Požadavek na rozvoj Objednatele
(2) Analýza Poskytovatele, vystavení nabídky a předání Objednateli
(3) Akceptace/zamítnutí nabídky Objednatelem
(4) V případě akceptace vystavení objednávky
(5) Proces aktualizace ISSV
(6) Akceptace plnění

Provoz IS

Aktualizace ISSV:

(1) Realizace důvodu aktualizace – změna legislativy, realizovaný rozvoj, nalezená bezpečnostní trhlina, nalezená chyba ISSV
(2) Příprava aktualizačního balíčku v prostředí Poskytovatele a testování
(3) Předání balíčku na Objednatele, předání changelogu a návrh nasazení balíčku
(4) Koordinace termínu nasazení aktualizace (mimo pracovní dobu)
(5) Nasazení za nezbytné součinnosti Poskytovatele infrastruktury
(6) Otestování funkčnosti Poskytovatelem
(7) Otestování funkčnosti Objednatelem
(8) Opětovné nasazení aktualizace v případě nálezů
(9) Nasazení bezchybné verze do produkce
(10) Aktualizace systémové dokumentace

Řešení nálezu/incidentu:

(1) Zjištění Objednatele, prvotní analýza ICT pracovníků Objednatele
(2) Nahlášení nálezu/incidentu Objednatelem do service-desku Poskytovatele infrastruktury a Poskytovatele

(3) Koordinace stran při hledání problému, pokud není jednoznačný
(4) Řešení nálezu/incidentu odpovědnou stranou
(5) Informování Objednatele o řešení
(6) Příprava aktualizačního balíčku dle SLA
(7) Proces Aktualizace ISSV

Rozvoj ISSV:

(7) Požadavek na rozvoj Objednatele
(8) Analýza Poskytovatele, vystavení nabídky a předání Objednateli
(9) Akceptace/zamítnutí nabídky Objednatelem
(10) V případě akceptace vystavení objednávky
(11) Proces aktualizace ISSV
(12) Akceptace plnění

V rámci poskytování služeb na objednávku (vč. rozvoje ISSV) během realizace ISSV (dodání Díla) v souladu se čl. 5.1 implementační smlouvy se předpokládá primární využití těchto služeb na objednávku na realizaci integrace na DCeGOV, případné realizace analýzy integrace a následného provedení integrace ISSV na alternativní dohledové centrum, vytvoření dodatečných formulářů a aktualizací funkcionalit ISSV a jejich implementaci dle požadavků vyplývajících z novel zákona o správě voleb; aktuálně se jedná o již platné zákony:

- **zákon č. 268/2024 Sb.** - předmětným zákonem je zaváděno korespondenční hlasování; má dílčí dopad na modul Seznamu voličů a provazby s Portálem občana,
- **zákon č. 269/2024 Sb.** - novela zákona o volbě prezidenta republiky a některých dalších zákonů, která má ve vztahu k ISSV věcný dopad na modul Nástroj ePetice.

Část životního cyklu vytváření IS je podrobněji popisována kapitolou Požadavky na řízení projektu Poskytovatelem a část Provoz IS kapitolou Požadavky na provozní podporu.

5.6. PROSTŘEDÍ

ISSV bude realizován v následujících prostředích. Pro každé prostředí bude existovat samostatná instance ISSV.

- Vývojové prostředí
- Testovací prostředí
- Preprodukční prostředí
- Produkční prostředí

Za vývojové prostředí ponese odpovědnost Poskytovatel a zajistí, že vývojové prostředí bude zabezpečeno do takové míry, aby nebyl možný únik dat nebo narušení integrity návrhu ISSV. Do vývojového prostředí bude Objednateli zřízen přístup přes VPN s využitím šifrovaného připojení. Tento síťový kanál bude otevřen vždy na vyžádání Objednatele (při kontrole či prezentaci postupu tvorby ISSV).

Testovací prostředí bude realizováno Poskytovatelem infrastruktury Objednatele za součinnosti Poskytovatele – Poskytovatel poskytne požadavky na testovací prostředí a při samotné implementaci

ISSV bude s Poskytovatelem infrastruktury spolupracovat. Pro testovací prostředí a testovací instanci ISSV platí stejné bezpečnostní požadavky jako pro produkční verzi. Testovací prostředí je realizováno s cílem otestování řešení ISSV a testování nových aktualizací ISSV, případně testování změn Objednatelem v oblasti dat a nastavení.

Preprodukční prostředí je realizováno jako kopie produkčního prostředí, tedy jak konfigurace, tak funkcionality a datový obsah budou identické. Preprodukční prostředí bude realizováno Poskytovatelem infrastruktury Objednatele a jeho cílem je testování chování ISSV, datových změn simulující produkční prostředí.

Produkční prostředí je bude realizováno Poskytovatelem infrastruktury Objednatele za součinnosti Poskytovatele – Poskytovatel poskytne požadavky na produkční prostředí dle výsledků performance testů a funkčních testů a při samotné implementaci ISSV bude s Poskytovatelem infrastruktury spolupracovat. Produkční prostředí slouží k poskytování samotných služeb ISSV koncovým uživatelům a pokrytí agend, které ISSV podporuje. Produkční prostředí, potažmo produkční instance ISSV je kritická z pohledu bezpečnosti, dostupnosti a zajištění fungování, neboť jeho nedostupnost, ohrožení či chybovost může vést k ohrožení přípravy nebo výkonu voleb.

5.7. INFRASTRUKTURA

Infrastruktura bude zajištěna Objednatelem a jeho Poskytovatelem infrastruktury. Detail je uveden v kapitole Technologická architektura.

5.8. OBECNÉ POŽADAVKY

- ISSV bude vytvářen s využitím aktuálních a bezpečných algoritmů, které nevykazují kybernetickou zranitelnost.
- V rámci tvorby ISSV bude aplikován princip security-by-design
- ISSV bude vytvářen jako optimalizovaný SW, nikoli SW s nedostatečnou kvalitou návrhu a zpracování na úrovni kódu a procesů s nutností kompenzace odezvy a výkonnosti takového SW nepřiměřenými systémový prostředky a požadavky na ně směrem k Objednateli či Poskytovateli infrastruktury Objednatele za účelem dodržení odezvy a funkcionality systému.
- ISSV s ohledem na předpokládaný dlouhodobý provoz a životnost pořizovaného řešení bude postaven na současných technologiích a kódování, které zajistí dlouhodobou funkčnost a podporu ISSV.
- ISSV bude využívat pro své UI doporučený Design systém gov.cz (https://designsystem.gov.cz/)
- ISSV bude přístupné webové responzivní SW řešení dle platné legislativy
- ISSV a všechny jeho části budou mít UI v českém jazyce, pro UI přihlášeného voliče bude k dispozici rovněž anglická jazyková mutace, pro veřejnou část bude k dispozici jako alternativní mutace rovněž anglický jazyk

6. POŽADAVKY NA BEZPEČNOST

6.1. OBECNÉ POŽADAVKY NA BEZPEČNOST

Objednatel je správcem informačních systémů kritické informační infrastruktury dle § 3 písm. c) ZOKB, správcem komunikačního systému kritické informační infrastruktury dle § 3 písm. d) ZOKB a správcem významných informačních systémů dle § 3 písm. e) ZOKB. Provádění plnění zakázky bude prováděno na aktivech systémů kritické informační infrastruktury a aktivech významných informačních systémů.

Objednatel chápe Poskytovatele jako významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 VoKB. Rozsah zajištění bezpečnosti Poskytovatelem je dán tímto dokumentem, smlouvou a jejími dalšími přílohami.

Poskytovatel je povinen naplnit bezpečnostní požadavky, dané kapitolou soulad s vyhláškou o kybernetické bezpečnosti do termínu uzavření smlouvy a nadále se jimi řídit po dobu realizace projektu i po dobu poskytování servisní podpory.

ISSV je budován jako ISVS, který je Objednatelem určen jako kritická informační infrastruktura dle zákona o kybernetické bezpečnosti. **V důsledku toho dodaný ISSV musí být bezpečné řešení v souladu se ZoKB, ISMS, VoKB a další platnou legislativou pro IS této klasifikace v ČR.**

Funkce ISSV lze volat výhradně v návaznosti na autentizaci a autorizaci uživatelů, služeb anebo aplikací. Autorizace se provádí jak v byznys vrstvě, tak i v aplikační vrstvě. SW administrátor a technické účty mají přístup k DB a aplikaci, proto jsou jejich aktivity monitorovány přes aplikační monitoring. Aktivita uživatelů musí být logována, logy musí být ukládány a současně vyhodnocovány v dohledovém centru Poskytovatele infrastruktury.

HW a technologickou bezpečnost zajišťuje Poskytovatel infrastruktury Objednatele. S ním je v oblasti kybernetické bezpečnosti Poskytovatel povinen spolupracovat pro odpovídající zajištění kybernetické bezpečnosti pro systém v klasifikaci KII.

6.2. IDENTIFIKACE BUSINESS HROZEB A ZRANITELNOSTÍ

Identifikace business hrozeb a zranitelností bude realizovaná Poskytovatelem a bude zpracovaná v rámci předimplementační analýzy – bezpečnostní část.

Poskytovatel v rámci identifikace odhalí možné hrozby externí i interní a identifikuje jejich možnosti ohrožení ISSV, jeho modulů, prostředí a databáze ISSV. Následně po identifikaci business hrozeb a zranitelností popíše scénáře ohrožení ISSV těmito hrozbami s ohodnocením dopadu na důvěrnost, dostupnost, integritu a dohledatelnost.

Kromě vyhodnocení těchto rizik bude Poskytovatel realizovat i vyhodnocení bezpečnosti aktiv s využitím doporučené podoby analýzy aktiv, poskytované NÚKIB. Vyhodnocení bezpečnosti aktiv bude postihovat ISSV, jeho prostředí, moduly a funkcionality, databázi a datové entity a vše s tím související. Vyhodnocení bude konzultovat s Objednatelem.

Analýzu rizik a hodnocení informačních aktiv bude Poskytovatel s Objednatelem rovněž realizovat ročně i v období provozu v rámci poskytování servisních služeb.

Poskytovatel omezí zranitelnost systému odstraněním vad, zjištěných v rámci penetračního testování ISSV, prováděného Objednatelem nebo smluvní stranou Objednatele. Při odstraňování zjištění musí Poskytovatel splnit smluvní termín odstranění vad.

Objednatel bude provádět roční penetrační testování svými kapacitami nebo smluvním partnerem i v období provozu a Poskytovatel je povinen odstranit nalezené vady v rámci poskytování servisních služeb.

6.3. POŽADAVKY NA DOSTUPNOST, DŮVĚRNOST A INTEGRITU DAT

Dostupnost bude zajištěna infrastrukturou v režimu vysoké dostupnosti. Dostupnost se však týká rovněž samotné aplikace ISSV a v případě, že ISSV je dostupný, nicméně nereaguje na uživatelskou interakci nebo vrací chybové hlášení, považuje se takový stav za aplikačně nedostupný IS. Stejně tak je za nedostupný považován takový stav, kdy není systém dostupný pro určité uživatele, avšak dostupný by měl být. V takovém případě platí, že pokud bude ze strany Poskytovatele infrastruktury vyloučena nedostupnost infrastruktury a technologické vrstvy, je nedostupnost považována za nedostupnost ISSV a vážou se na ní SLA dostupnosti informačního systému, definované v této technické specifikaci. Poskytovatel je tedy povinen zajistit aplikačními prostředky deklarovanou dostupnost dle SLA této technické specifikace. Pro zajištění dostupnosti platí požadavek, že ISSV a všechny jeho funkcionality vč. Standardního SW budou dostupné pro přístup on-premise v síti CMS 2.0. i při nedostupnosti veřejné sítě internet. Tento požadavek bude testovaný jak při realizaci Díla, tak ročně během provozu.

Důvěrnost bude zajištěna přístupem na základě důvěryhodné autentizace (NIA, JIP/KAAS, CAAIS) a přiřazením odpovídající role v informačním systému. Důvěrnost dat rovněž podporuje šifrování komunikace a zajištění bezpečnostním softwarem Poskytovatele infrastruktury. ISSV musí zajistit důvěrnost dat s přístupem pouze oprávněnému uživateli. Přístupy budou logované, vč. ID uživatele a vykonávaných operací.

Integrita dat bude zajištěna šifrovanými přenosy a omezením uživatelských akcí dle jejich rolí. Systém musí zajistit datovou integritu na úrovni databáze jejím monitoringem a logováním přístupů do DB, zápisů a změn.

Poskytovatel stanoví v rámci předimplementační analýzy bezpečnost a architekturu ISSV tak, aby byla zajištěna aplikační dostupnost, důvěrnost, integrita a dohledatelnost jak akcí, tak samotných dat.

6.4. POŽADAVKY NA LOGOVÁNÍ UDÁLOSTÍ A BEZPEČNOSTNÍ MONITORING

ISSV bude Poskytovatelem napojen na dohledové centrum Objednatele, případně i dohledové centrum Poskytovatele infrastruktury Objednatele.

Systém a všechny použité komponenty (včetně Standardního SW) budou naplňovat požadavky na logování událostí dle § 5 ZoKB a § 22 VoKB.

ISSV, stejně jako veškeré komponenty, ze kterých se skládá ISSV (včetně Standardního SW) tedy musí mít nastaveno logování na patřičné úrovni pro naplnění zmiňovaných požadavků ZoKB a Vyhlášky § 22, zejména následující požadavky VoKB:

(2) Povinná osoba pro zaznamenávání bezpečnostních a provozních událostí podle odstavce 1 zajišťuje

b) sběr informací o bezpečnostních a provozních událostech; zejména zaznamenává

1. **datum a čas včetně specifikace časového pásma,**

2. **typ činnosti,**

3. **identifikaci technického aktiva, které činnost zaznamenalo,**

4. **jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,**

5. **jednoznačnou síťovou identifikaci zařízení původce a**

6. **úspěšnost nebo neúspěšnost činnosti,**

d) zaznamenávání

1. **přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,**
2. **činností provedených administrátory,**
3. **úspěšné i neúspěšné manipulace s účty, oprávněními a právy,**
4. **neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,**
5. **činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,**
6. **zahájení a ukončení činností technických aktiv,**
7. **kritických i chybových hlášení technických aktiv a**
8. **přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí a**

Zároveň na úrovni ISSV musí být zajištěno splnění souvisejících podmínek jako je:

(1) Povinná osoba

b) **na základě hodnocení důležitosti aktiv aktualizuje rozsah aktiv, u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno**.

(2) Povinná osoba pro zaznamenávání bezpečnostních a provozních událostí podle odstavce 1 zajišťuje

c) **ochranu informací získaných podle písmen a) a b) před neoprávněným čtením a jakoukoli změnou,**

e) **synchronizaci jednotného času technických aktiv nejméně jednou za 24 hodin.**

(3) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona **uchovává záznamy událostí** zaznamenaných podle odstavce 2 **nejméně po dobu 18 měsíců.**

Poskytovatel pro zajištění výše uvedených požadavků na logování událostí na úrovni ISSV a jeho komponent bude spolupracovat s Poskytovatelem infrastruktury Objednatele a Objednatelem.

Pro ISSV jakožto KII tedy platí, že všechny komponenty od úrovně HW přes virtualizaci, OS, databáze, aplikační SW, ale i podpůrná aktiva daného IS jako jsou zálohovací služby apod., musí mít patřičně nastaveno logování, minimálně jednou za 24 hodin synchronizovaný čas a musí být zajištěna ochrana takovýchto logových záznamů pro splnění podmínky VoKB odstavce (2) písmene c), přičemž vše výše uvedené platí i pro data získaná dle odstavce (2) písmeno d). Na úrovni ISSV je za uvedené odpovědný Poskytovatel.

Při jakékoli změně ISSV, jeho aktualizaci nebo rozvoji musí Poskytovatel analyzovat dopad změn na rozsah logovaných informací a událostí a v případě dopadu na rozsah logovaných informací rozšířit/modifikovat rozsah logování tak, aby byl ISSV, vč. nových/změněných funkcionalit plně logovaný.

V rámci logování musí být zajištěna integrita informací pomocí adekvátních kryptografických prostředků definovaných Poskytovatelem infrastruktury Objednatele nebo Objednatelem, aby bylo možné jednoznačně určit, kdo logovanou operaci provedl.

Poskytovatel je povinen zajistit logování všech akcí dle výše uvedených požadavků a tyto logy se zajištěním jejich integrity a synchronního času přenést do dohledového centra Poskytovatele infrastruktury Objednatele či rovněž Objednatele.

6.5. DETEKCE, PREVENCE A ZVLÁDÁNÍ INCIDENTŮ

Poskytovatel v rámci předimplementační analýzy stanoví procesy, organizační role vč. odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů, podle takto

stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Objednateli prostřednictvím nastavených komunikačních kanálu a v případech, kdy situace nestrpí odklad prostřednictvím telefonu.

Ve všech případech bude rovněž spolupracovat s Poskytovatelem infrastruktury Objednatele, který bude zajišťovat bezpečnostní monitoring na infrastrukturní a technologické úrovni a metodické postupy Poskytovatele budou v souladu s postupy Poskytovatele infrastruktury, která bude zajišťovat bezpečnostní monitoring a bezpečnost infrastruktury.

Nastavená pravidla pro zvládání bezpečnostních incidentů budou respektovat požadavek na legalitu zajištění stop, tj. jejich původ a oprávněnost jejich získaní musí být v souladu s platnými zákony a standardy tak, aby bylo možné jejich následné využití v rámci forenzní analýzy a eventuální použití jako důkazní materiál.

Prevence incidentů bude dána jak pravidelným testování, tak analýzou rizik a aktivně s využitím SW SIEM Poskytovatele infrastruktury Objednatele.

V oblasti bezpečnostních incidentů je Poskytovatel povinen poskytnout spolupráci jak Objednateli, tak Poskytovateli infrastruktury Objednatele v souladu s ISMS Objednatele a postupy stanovenými v rámci předimplementační analýzy a dokumentaci ISSV.

6.6. POŽADAVKY NA SYSTÉMOVOU BEZPEČNOST

Systém bude již **při vývoji vytvářen Poskytovatelem jako bezpečný s architekturou security-by-design**. Tedy již zdrojové kódy budou vytvářeny tak, aby vykazovaly nízkou míru zranitelnosti.

Systémová architektura ISSV bude reflektovat doporučení NÚKIB, ISMS, ZoKB a doporučení bezpečnostní organizační složky Objednatele s cílem minimalizace ohrožení bezpečnostními událostmi.

Systémová bezpečnost bude kombinovaná, zajištění ochrany bude zajištěno bezpečným kódováním ISSV a využitím aktuálních kryptografických prostředků s dohledem a bezpečnostním SW Poskytovatele infrastruktury Objednatele.

Systémová bezpečnost bude rovněž zajištěna návrhem bezpečné architektury ISSV, nastavením procesů v oblasti bezpečnosti, které musí korespondovat s ISMS a procesy Objednatele, pravidelným penetračním testováním a analýzou rizik pro systém vč. aktualizace klasifikace aktiv.

Systém a všechny jeho komponenty (vč. Standardních SW) musí mít zajištěny bezpečnostní aktualizace se zajištěním podpory bezpečnosti Systému a jeho komponent v rámci servisních služeb Poskytovatele/výrobce SW.

6.7. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

S osobními údaji bude zacházeno v souladu s platnou legislativou. Poskytovatel nebude mimo schválené úložiště Objednatelem a Poskytovatelem infrastruktury Objednatele nikde ukládat data ani osobní údaje a v případě, že data obsahují osobní údaje, musí s nimi systém zacházet v souladu s požadavky legislativy.

Bezpečnost osobních údajů bude zajištěna ze strany Poskytovatele infrastruktury odděleným uložením s monitorovaným a řízeným přístupem a bezpečnostními opatřeními na úrovni tohoto úložiště. **Tuto architekturu musí rovněž reflektovat architektura ISSV a v případě, že systém operuje s osobními údaji, musí zajistit důvěrnost a integritu těchto osobních údajů.**

Poskytovatel je povinen řídit se při zpracování Osobních údajů rovněž ustanoveními p**řílohy č. 10 smlouvy a přílohy 9 servisní smlouvy.** Poskytovatel mimo jiné poskytne dostatečné záruky o technickém a organizačním zabezpečení ochrany Osobních údajů.

Poskytovatel je povinen informovat Objednatele (správce osobních údajů) o každém případu ztráty či úniku Osobních údajů, neoprávněné manipulace s Osobními údaji nebo jiného porušení zabezpečení Osobních údajů („**Porušení zabezpečení osobních údajů**"), a to bez zbytečného odkladu, nejpozději do čtyřiadvaceti (24) hodin od vzniku Porušení zabezpečení osobních údajů nebo i pouhé hrozby.

Poskytovatel bude Objednateli nápomocen při zajišťování povinností dle Nařízení o ochraně osobních údajů, především povinnosti zabezpečit zpracování Osobních údajů, ohlašovat případy Porušení zabezpečení osobních údajů, **zajištění posouzení vlivu na ochranu Osobních údajů** či konzultací s ÚOOÚ.

Poskytovatel pro ochranu osobních údajů přijme minimálně následující organizační a technická opatření:

- v případě zpracování osobních údajů prostřednictvím vlastních zaměstnanců pověří touto činností pouze své vybrané zaměstnance a členy realizačního týmu, které zaváže povinností mlčenlivosti ohledně osobních údajů a zaváže je k dodržování dalších povinnosti, které jsou povinni dodržovat tak, aby nedošlo k porušení platné legislativy či přílohy č. 10 smlouvy, **přílohy 9 servisní smlouvy**, a to například v rámci interního předpisu Zpracovatele, dohodě o mlčenlivosti či v pracovní smlouvě zaměstnance
- využije odpovídající technické zařízení a programové vybavení způsobem, který vyloučí neoprávněný či nahodilý přístup k osobním údajům ze strany jiných osob než pověřených osob Poskytovatele
- bude osobní údaje uchovávat v náležitě zabezpečených objektech a místnostech v případě uložení mimo prostory Objednatele
- Osobní údaje v elektronické podobě bude Poskytovatel uchovávat na zabezpečených serverech nebo na nosičích dat, ke kterým budou mít přístup pouze pověřené osoby Poskytovatele na základě autentizace, a bude osobní údaje pravidelně zálohovat, pokud takové zálohy neprovádí Objednatel
- zabezpečí dálkový přenos osobních údajů buď pouze prostřednictvím veřejně nepřístupné sítě, nebo prostřednictvím zabezpečeného přenosu po veřejných sítích s využitím odpovídajících kryptografických prostředků
- písemné dokumenty obsahující osobní údaje bude uchovávat na zabezpečeném místě, přičemž bude vést řádnou evidenci o pohybu takových písemných dokumentů
- bude v co největší míře zpracovávat pouze pseudonymizované a šifrované osobní údaje, kde to uložení umožní a je-li takové opatření vhodné a nezbytné ke snížení rizik ply,wnoucích ze zpracování osobních údajů
- zabezpečí neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování osobních údajů;
- prostřednictvím vhodných technických prostředků zabezpečí schopnost obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů (jako součást DRP);
- zabezpečí pravidelné testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování osobních údajů

Při ukončení zpracování osobních údajů zabezpečí Poskytovatel dle dohody s Objednatelem výmaz osobních údajů, nebo tyto osobní údaje předá Objednateli dle přílohy č. 10 smlouvy **a přílohy 9 servisní smlouvy.**

Pokud Objednatel **na základě provedení posouzení vlivu na ochranu osobních údajů** dojde k závěru, že je nezbytné provést další opatření, nestanovené v tomto dokumentu, smlouvě nebo příloze č. 10 smlouvy **či příloze 9 servisní smlouvy**, je Poskytovatel povinen taková opatření realizovat a následně bude opatření zaznamenáno do smlouvy formou dodatku.

6.8. NAPLŇOVÁNÍ SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Poskytovatel je povinen se při realizaci Díla řídit dokumentací Systému řízení bezpečnosti informací Objednatele (politikami ISMS) a poskytovat Objednateli součinnost na vyžádání při jejich naplňování.

V rámci realizace Díla Poskytovatel vytvoří dokumentaci v souladu s požadavky Systému řízení bezpečnosti informací dle následujícího výčtu:

- Bezpečnostní politika pro ISSV
- Plán zvládání rizik
- Prohlášení o aplikovatelnosti
- Plán kontinuity činností
- Zpráva o hodnocení aktiv a rizik

Pro vytvoření výše uvedené dokumentace využije Poskytovatel šablony, které mu budou poskytnuty Objednatelem. Objednatel dále poskytne Poskytovateli nezbytnou součinnost při vytváření dokumentace.

Pro vytvoření zprávy o hodnocení aktiv a rizik bude Poskytovatelem realizována analýza aktiv a rizik pro ISSV a všechny jeho části vč. standardního SW. Součástí analýzy bude vyhodnocení rizik dle varování Národního úřadu pro kybernetickou a informační bezpečnost vydaným podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

Poskytovatel má právo vyžádat si od Objednatele dokumenty (politiky ISMS) centrální dokumentace Systému řízení bezpečnosti informací resortu Ministerstva vnitra, které mu budou Poskytovateli předány na základě Dohody o zachování mlčenlivosti o důvěrných informacích (NDA). Jedná se např. o následující dokumenty ISMS resortu MV:

ISMS 02.03 Řízená dokumentace

- ISMS 02.03.01 Řízení dokumentů a záznamů
- ISMS 02.03.01.P01 Šablona řízeného dokumentu Word
- ISMS 02.03.01.P02 Řízení vzniku a změn dokumentů
- ISMS 02.03.01.P03 Rušení dokumentů
- ISMS 02.03.01.P04 Šablona řízeného dokumentu Excel
- ISMS 02.03.01.P05 Šablona řízeného dokumentu Word na šířku
- ISMS 02.03.01.P06 Šablona řízeného dokumentu Powerpoint
- ISMS 02.03.01.P07 Šablona řízeného dokumentu Powerpoint 16-9
- ISMS 02.03.02 Zkratky a pojmy ISMS MV

ISMS 02.10 Quick Guide ISMS

- ISMS 02.10.03.P01 Šablona bezpečnostní politiky
- ISMS 02.10.03.P01.P01 Šablona matice související dokumentace
- ISMS 02.10.03.P04 Šablona plánu zvládání rizik
- ISMS 02.10.03.P05 Šablona zprávy o hodnocení aktiv a rizik
- ISMS 02.10.03.P07 Šablona evidence změn
- ISMS 02.10.03.P13 Šablona plánu řízení KBI
- ISMS 02.10.03.P14 Šablona plán kontinuity činností a obnovy
- ISMS 02.10.03.P16 Šablona identifikace a hodnocení primárních aktiv
- ISMS 02.10.03.P22 Šablona MS k hodnocení aktiv a rizik
- ISMS 02.10.04 Bezpečnostní doporučení pro administrátory ICT resortu MV

ISMS 03.01 Bezpečnostní politiky

- ISMS 03.01.01 Politika řízení dodavatelů
- ISMS 03.01.02 Politika řízení aktiv a rizik
- ISMS 03.01.02.P01 Metodika identifikace a hodnocení aktiv a rizik
- ISMS 03.01.02.P01.P01 Proces hodnocení aktiv a rizik
- ISMS 03.01.04 Politika řízení provozu a komunikací
- ISMS 03.01.05 Politika řízení přístupu
- ISMS 03.01.05.P01 Pravidla vzdáleného přístupu
- ISMS 03.01.06 Politika bezpečného chování uživatelů
- ISMS 03.01.07 Politika zálohování a obnovy a dlouhodobého ukládání
- ISMS 03.01.08 Politika bezpečného předávání a výměny informací
- ISMS 03.01.09 Politika řízení technických zranitelností
- ISMS 03.01.10 Politika bezpečného používání mobilních zařízení a médií
- ISMS 03.01.11 Politika akvizice, vývoje a údržby
- ISMS 03.01.11.P01 Postup připojení IS do DCeGOV
- ISMS 03.01.11.P01.P01 Doporučené nastavení logování technologických komponent
- ISMS 03.01.11.P01.P02 ArcSight podporované produkty
- ISMS 03.01.11.P01.P03 Evidence poskytování událostí – šablona
- ISMS 03.01.13 Politika fyzické bezpečnosti
- ISMS 03.01.13.P01 Bezpečnost datových center
- ISMS 03.01.14 Politika bezpečnosti komunikační sítě
- ISMS 03.01.15 Politika ochrany před škodlivým kódem
- ISMS 03.01.16 Politika nasazení a používání nástroje pro detekci KBU
- ISMS 03.01.17 Politika využití a údržby nástroje pro sběr a vyhodnocení KBU
- ISMS 03.01.18 Politika bezpečného používání kryptografické ochrany
- ISMS 03.01.18.P01 Minimální požadavky na kryptografické algoritmy
- ISMS 03.01.19 Politika řízení změn
- ISMS 03.01.19.P01 Evidence změn – vzor

- ISMS 03.01.20 Politika zvládání KBU a KBI
- ISMS 03.01.20.P01 Kategorizace incidentů
- ISMS 03.01.21 Politika řízení kontinuity činností
- ISMS 03.01.21.P01 Plán řízení KBI – vzor
- ISMS 03.01.21.P02 Plán kontinuity činností a obnovy – vzor
- ISMS 03.01.24 Politika správy životního cyklu domén a doménových certifikátů

6.9. SOULAD S VYHLÁŠKOU O KYBERNETICKÉ BEZPEČNOSTI

Poskytovatel bude v rámci plnění zakázky dodržovat požadavky Vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (VoKB) a poskytovat Objednateli součinnost pro plnění povinností z VoKB vyplývajících.

V rámci plnění je rovněž vyžadováno, aby se Poskytovatel řídil povinnostmi, které Objednatel prosazuje v rámci zavedeného systému řízení bezpečnosti informací (ISMS dle ISO 27001).

Poskytovatel se zavazuje dodržovat následující povinnosti, které jsou rovněž uvedeny jako součást smlouvy k zakázce.

6.9.1. SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 3 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění této zakázky.

Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění této zakázky, monitorovat je, vyhodnocovat jejich účinnost.

Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění této zakázky, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.

Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění této zakázky. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.

Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

Poskytovatel je dále povinen dodržovat bezpečnostní politiku Objednatele, byl-li s ní seznámen.

6.9.2. ŘÍZENÍ AKTIV

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 4 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této zakázky (aktivy se rozumí např. data a informace k předmětu plnění dle této zakázky, systémy ICT, moduly, hardware prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli

předložit do třiceti (30) dnů od platnosti této zakázky a následně na vyžádání, a to po celou dobu trvání smlouvy a po dobu dvou (2) let po jejím ukončení.

6.9.3. ŘÍZENÍ RIZIK

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 5 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění této zakázky.

V minimálním intervalu 1x ročně vytvořit a předložit Objednateli zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:

- Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;
- Identifikaci a hodnocení rizik s vazbou na předmět plnění;
- Realizovaná bezpečnostní opatření;
- Nepokrytá bezpečnostní rizika a návrh opatření;
- Vyhodnocení bezpečnostních událostí a incidentů; a
- Aktuální stav souladu Poskytovatele s Kybernetickými požadavky.

6.9.4. ORGANIZAČNÍ BEZPEČNOST

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 6 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

V souladu s Článkem 28 smlouvy jmenovat odpovědnou Kontaktní osobu pro kybernetickou bezpečnost pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi Stranami.

Využívat pro poskytování předmětu plnění této zakázky pouze oprávněných osob, které byly řádně seznámeny s příslušnými Interními předpisy Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

6.9.5. ŘÍZENÍ PODDODAVATELŮ

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 8 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Využívá-li při poskytování předmětu plnění této zakázky Poddodavatele, zabezpečit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými Poddodavateli, přičemž tuto skutečnost se Poskytovatel zavazuje doložit Objednateli do deseti (10) dnů od uzavření příslušné smlouvy, na jejímž plnění se budou Poddodavatelé podílet, písemným prohlášením Poskytovatele o dodržování Kybernetických požadavků u svých Poddodavatelů.

Pokud při poskytování předmětu plnění dochází ke zpracování Osobních údajů, zabezpečit nad rámec Článku 16 smlouvy uzavření samostatných smluv (tj. smluv se svými Poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění) ve smyslu příslušných ustanovení Nařízení.

6.9.6. BEZPEČNOST LIDSKÝCH ZDROJŮ

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 9 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

zabezpečit, aby Kontaktní osoba pro kybernetickou bezpečnost nejpozději do třiceti (30) dnů od platnosti smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování

předmětu plnění této zakázky za Poskytovatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními Interních předpisů Objednatele.

Dodržovat příslušná ustanovení Interních předpisů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Poskytovatel zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné Interní předpisy.

V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění této zakázky.

Zabezpečit, aby osoby podílející se na poskytování plnění této zakázky v IT prostředí objednatele anebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo IT prostředí objednatele:

- Pro uložení a sdíleni dat a informací Objednatele využívali pouze k tomu schválené prostředky (aktiva) a schválené způsoby komunikace;
- Neukládali ani nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
- Nestahovali, nesdíleli, neukládali, nearchivovali ani neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo předpisy upravující ochranu duševního vlastnictví;
- Nenavštěvovali internetové stránky s eticky nevhodným obsahem;
- Nerealizovali pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů; a
- Nerealizovali pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;
- Nepodíleli se s prostředky Objednatele na šíření spamu ani škodlivého Softwaru;
- Dodržovali obecně závazné právní předpisy.

Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je zpracování Osobních údajů pověřených osob Poskytovatele, kteří se podílejí na zajištění předmětu plnění této zakázky. Pokud nebude Objednateli umožněno Osobní údaje dotčených pověřených osob Poskytovatele zpracovat, nebude těmto pověřeným osobám umožněn žádný přístup ke zdrojům Objednatele.

6.9.7. ŘÍZENÍ PROVOZU A KOMUNIKACÍ

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 10 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Zabezpečit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění této zakázky.

Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

Zabezpečit, že pro poskytování předmětu plnění této zakázky budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví.

6.9.8. ŘÍZENÍ ZMĚN

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 11 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

Aktivně spolupracovat při testování významné změny.

6.9.9. ŘÍZENÍ PŘÍSTUPU

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 12 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Přidělovat oprávnění svým jednotlivým pověřeným osobám ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.

Zabezpečit, aby udělený přístup nebyl sdílen více osobami Poskytovatele, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Poskytovatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání této zakázky a dva (2) roky po jejím ukončení.

Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k IT prostředí objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).

Zabezpečit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům Objednatele (IT prostředí objednatele) chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do IT prostředí Objednatele.

Poskytovatel bere na vědomí, že přístup k IT prostředí objednatele je možné povolit pouze fyzické identitě zaměstnance Poskytovatele / Poddodavatele, a to na základě požadavku Poskytovatele na přístup těchto osob.

Poskytovatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.

Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby na straně Poskytovatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Objednatele).

6.9.10. AKVIZICE, VÝVOJ A ÚDRŽBA

Poskytovatel se bude v rozsahu předmětu plnění této zakázky aktivně podílet na splnění povinností uvedených v § 13 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Zabezpečit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění smlouvy k této zakázce, ledaže tyto činnosti provádí Objednatel.

Předat Objednateli v přiměřené lhůtě stanovené Objednatelem dokumentaci předmětu plnění smlouvy k této zakázce minimálně v následujícím rozsahu:

- dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
- dokumentaci obsahující popis autorizačního konceptu a oprávnění;
- dokumentaci obsahující instalační a konfigurační postupy.

V případě, že předmět plnění této zakázky zahrnuje vývoj Softwaru, zavazuje se Poskytovatel:

- Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj Softwaru v závislosti na charakteru plnění.
- Na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit Objednateli vyvíjený Zdrojový kód na provedení codereview anebo výstupy z provedeného codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně) po jeho dokončení, pokud není v této smlouvě stanoveno jinak, a to zejména za účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito Kybernetickými požadavky.
- Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje Softwaru či kdykoli po jeho předání.
- Zabezpečit, že plnění této zakázky bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování Softwaru anebo které jsou specifikovány výslovně v smlouvě (zejména, že Software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).
- Pokud je součástí plnění této zakázky i instalace operačního systému případně Softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Objednatele.
- Zabezpečit bezpečnost testovacího prostředí u Poskytovatele (pokud testovací prostředí neprovozuje Objednatel) a ochranu testovacích dat poskytnutých Objednatelem.
- Zabezpečit, že do produkčního prostředí Objednatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný Zdrojový kód a další nezbytná data pro provozování předmětu plnění této zakázky.
- Zabezpečit, že v rámci poskytovaného plnění smlouvy k této zakázce bude dodávaný Software:
    - v souladu s bezpečnostními politikami a standardy Objednatele (Interními předpisy – především zavedeným ISMS); a
    - otestován na soulad s bezpečnostními politikami Objednatele (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami (Interními předpisy) seznámen).
- Instalovat Software pouze na základě Objednatelem předem schválených migračních postupů.
- Předat Zdrojový kód Objednateli bezpečnou formou zajišťující jeho integritu.
- Zabezpečit řízení verzí Zdrojového kódu.
- Zabezpečit zálohování Zdrojového kódu a jeho uložení mimo produkční prostředí.

- Zabezpečit, aby distribuce Zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto Zdrojových kódů.
- Nevyvíjet, nekompilovat a nešířit v prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

6.9.11. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

Poskytovatel se bude v rozsahu předmětu plnění smlouvy k této zakázce aktivně podílet na splnění povinností uvedených v § 14 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.

Bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby pro kybernetickou bezpečnost.

Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu anebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Poskytovatele.

Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.

Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující povinnost k náhradě újmy Poskytovatele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Poskytovatele za prodlení obsažená v smlouvě nejsou tímto ustanovením dotčena.

6.9.12. ŘÍZENÍ KONTINUITY ČINNOSTÍ

Poskytovatel se bude v rozsahu předmětu plnění smlouvy k této zakázce aktivně podílet na splnění povinností uvedených v § 15 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění smlouvy k této zakázce.

Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně Plnění.

6.9.13. KONTROLA A AUDIT

Poskytovatel se bude v rozsahu předmětu plnění smlouvy k této zakázce aktivně podílet na splnění povinností uvedených v § 8 a § 16 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany NÚKIB dle § 23 ZOKB.

6.9.14. FYZICKÁ BEZPEČNOST

Poskytovatel se bude v rozsahu předmětu plnění smlouvy k této zakázce aktivně podílet na splnění povinností uvedených v § 17 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče (Interní předpisy).

V rozsahu předmětu plnění smlouvy k této zakázce zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv Objednatele, pokud s ní byl Poskytovatel seznámen.

6.9.15. BEZPEČNOSTNÍ NÁSTROJE

Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 18 až § 27 VoKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

Realizovat bezpečnostní opatření pro odstranění anebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity a bezpečnosti komunikační sítě.

Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.

Připojovat do IT prostředí objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele.

Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Poskytovatele.

Na aktiva Objednatele neinstalovat a nepoužívat v IT prostředí objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění smlouvy k této zakázce:

- Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
- Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.
- Analyzátor zranitelností (scanner zranitelností) – softwarový anebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.
- Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.
- Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.

Připojovat do IT prostředí objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.

Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné a účinné české a evropské legislativy.

Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění smlouvy k této zakázce, a to po celou dobu trvání smlouvy a dobu poskytování servisních služeb.

Zabezpečit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění smlouvy k této zakázce a ochranu získaných informací před jejich neoprávněným čtením anebo změnou.

Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.

Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

Poskytovatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Poskytovatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud smlouva k této zakázce nestanoví jinak.

7. LEGISLATIVNÍ POŽADAVKY

7.1. POŽADAVKY NA SOULAD S LEGISLATIVOU ICT

Poskytovatel je v rámci realizace projektu, ale rovněž při poskytování servisních služeb povinen sledovat aktuální legislativu, vztaženou k ISSV. Mimo jiné je povinen sledovat mimo jiné následující právní předpisy ve znění pozdějších předpisů.

Poskytovatel je povinen seznámit se s povinnostmi Objednatele souvisejícími s ISSV a vyplývajícími z právních předpisů, tyto povinnosti průběžně sledovat a udělovat Objednateli doporučení v souladu se smlouvou a servisní smlouvou.

ISSV bude zcela v souladu s platnou legislativou platnou pro ISVS v režimu kritické infrastruktury státu. Především bude v souladu s:

- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- zákon č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
- nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů
- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů
- nZOKB – NIS2
- zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), v aktuálním znění
- zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů
- vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci
- vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy
- a veškerou další neuvedenou relevantní platnou legislativou v oblasti eGovernmentu a ICT státu

7.2. POŽADAVKY NA SOULAD S VĚCNOU LEGISLATIVOU

ISSV bude v souladu s platnou věcnou legislativou:

- Zákon č. 88/2024 Sb., o správě voleb, ve znění pozdějších předpisů

- zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 130/2000 Sb., o volbách do zastupitelstev krajů a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně a doplnění některých dalších zákonů, ve znění pozdějších předpisů
- zákon č. 275/2012 Sb., o volbě prezidenta republiky a o změně některých zákonů (zákon o volbě prezidenta republiky), ve znění pozdějších předpisů
- zákon č. 62/2003 Sb., o volbách do Evropského parlamentu a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 22/2004 Sb., o místním referendu a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 118/2010 Sb., o krajském referendu a o změně některých zákonů, ve znění pozdějších předpisů
- zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů
- zákon č. 129/2000 Sb., o krajích (krajské zřízení), ve znění pozdějších předpisů
- zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
- zákon č. 424/1991 Sb., o sdružování v politických stranách a v politických hnutích, ve znění pozdějších předpisů
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- zákon č 110/2019 Sb., o zpracování osobních údajů
- nařízení Evropského parlamentu a Rady (EU) č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu
- vyhláška č. 59/2002 Sb., o provedení některých ustanovení zákona č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů, ve znění pozdějších předpisů
- vyhláška č. 152/2000 Sb., o provedení některých ustanovení zákona č. 130/2000 Sb., o volbách do zastupitelstev krajů a o změně některých zákonů, ve znění pozdějších předpisů
- vyhláška č. 233/2000 Sb., o provedení některých ustanovení zákona č. 247/1995 Sb., o volbách do Parlamentu České republiky a o změně některých zákonů, ve znění zákona č. 212/1996 Sb., nálezu Ústavního soudu uveřejněného pod č. 243/1999 Sb. a zákona č. 204/2000 Sb., ve znění pozdějších předpisů
- vyhláška č. 294/2012 Sb., o provedení některých ustanovení zákona o volbě prezidenta republiky, ve znění pozdějších předpisů
- vyhláška č. 409/2003 Sb., k provedení zákona č. 62/2003 Sb., o volbách do Evropského parlamentu a o změně některých zákonů, ve znění pozdějších předpisů

- směrnice rady 93/109/ES ze dne 6. prosince 1993, kterou se stanoví pravidla pro výkon práva volit a být volen ve volbách do Evropského parlamentu občanů Unie, kteří mají bydliště v některém členském státě a nejsou jeho státními příslušníky
- sdělení č. 51/2015 Sb.m.s., o sjednání Úmluvy o účasti cizinců na veřejném životě na místní úrovni
- a veškerou další neuvedenou relevantní platnou legislativou v oblasti voleb ČR

8. POŽADAVKY NA TESTOVÁNÍ

8.1. POŽADOVANÉ TESTY

ISSV bude pravidelně testován, a to při realizaci Díla, ale i po dobu poskytování servisních služeb. V rámci testování ISSV bude Poskytovatelem realizovaná minimálně níže uvedená série testů. Testy budou realizovány v následujících obdobích:

- Po ukončení vývoje ve vývojovém prostředí Poskytovatele – realizátor testování je Poskytovatel
- Po nasazení ISSV do testovacího prostředí a jeho konfiguraci – realizátorem testování je Poskytovatel či Objednatel (penetrační testy), případně v kombinaci testerů (na uživatelských aplikačních testech a UX/UI testech)
- Po nasazení ISSV v produkčním a preprodukčním prostředí – realizátorem testování je Poskytovatel či Objednatel (penetrační testy), případně v kombinaci testerů (na uživatelských aplikačních testech a UX/UI testech)

Testování, jenž bude realizované Poskytovatelem, se budou moci od fáze nasazení ISSV do testovacího provozu účastnit na vyžádání zástupci Objednatele a jeho partnerů v roli pozorovatele.

Ze všech testování bude k dispozici testovací protokol, a to platí i pro víceiteranční testování, kdy pro každou iteraci bude existovat testovací protokol.

Protokol bude shrnovat testované oblasti, využité metody testování, uvedení testerů, průběh testování, výsledky testování a zjištění z testování. Protokoly budou vždy po jejich vyhotovení předány Objednateli a odprezentovány na projektové poradě.

Objednatel si vyhrazuje právo od fáze nasazení ISSV do testovacího provozu realizovat vlastní testy, přičemž zjištění z těchto testů následně předá Poskytovateli a budou-li součástí zjištění neoptimalit či chyb, je Poskytovatel **povinen tyto zjištění napravit ve stejném režimu jako zjištění z testů, realizovaných Poskytovatelem.**

Testování bude v případě nálezů z testování opakované (víceiterační), a to až do vyhodnocení testu bez nálezu. Ve všech iteracích musí Poskytovatel realizovat test či poskytnou součinnost v případě testu realizovaném Objednatelem či třetí stranou zajištěnou Objednatelem.

V případě nálezu chyby ISSV je za opakované testování a s tím související časový posun odpovědný Poskytovatel a musí jej dále kompenzovat na vlastní náklad pro zajištění kvality a termínu dodání Díla (např. zajištěním více HR kapacit v dalších etapách apod.).

8.1.1. UŽIVATELSKÉ APLIKAČNÍ TESTY

Uživatelské aplikační testy budou postihovat práci uživatelů v jednotlivých rolích v ISSV, definovaných v business architektuře řešení ISSV. Uživatelské aplikační testy budou testovat všechny procesy, které daná role bude v ISSV vykonávat.

8.1.2. UX/UI TESTY

UX/UI testy budou realizovány za účasti Objednatele a bude sledována uživatelské rozložení, přívětivost s cílem nalezení možných neoptimalit UI jednotlivých prostředí. V případě nalezení bude toto zjištění napraveno. Přestože bude ISSV navržen Poskytovatelem s využitím doporučených knihoven a UI design.gov, je zapotřebí test provést. Součástí UX/UI bude ověření přístupnosti ISSV v případě, že došlo ke změnám vůči knihovnám design.gov.

8.1.3. FUNKČNÍ TESTY

Funkční testy budou realizovány Poskytovatelem za dohledu Objednatele. Cílem je testování funkcionalit ISSV – modulů, jejich funkcí, konfigurace, integrací a datových přenosů, zápisů a čtení databáze atd. Součástí bude otestování administrátorských funkcí, tohoto testování se budou moc účastnit vybraní pracovníci Objednatele v roli testerů.

Funkční testy slouží k ověření fungování ISSV, správy ISSV, funkcí ISSV a všech aplikačních procesů. Součástí bude ověření fungování aplikace a jejích komponent v síti CMS 2.0. bez přístupu k veřejnému internetu.

8.1.4. PERFORMANCE TESTY

Performance testy budou realizovány Poskytovatelem za nezbytné součinnosti Poskytovatele infrastruktury Objednatele.

Performance testy budou nejprve realizovány Poskytovatelem ve vývojovém prostředí pro upřesnění nároků ISSV na kapacitní výkon a testy mohou odhalit rovněž performance neoptimality (opakované cyklené požadavky či jiné).

Performance testy na testovacím a produkčním prostředí budou realizované ve spolupráci s Poskytovatelem infrastruktury Objednatele. Pro ověření testování budou užity monitorovací nástroje infrastruktury Poskytovatele infrastruktury a monitorovací nástroje ISSV.

V rámci performance testů bude testována odezva – simulace operací se zvyšujícím se počtem paralelních operací s monitoringem odezvy v ms a dostupnost během testování při opakovaných požadavcích až do krajního přetížení systému a ztráty dostupnosti nebo neudržitelné odezvy systému nad 10000ms.

Performance testy budou minimálně testovat:

- Vysokou dostupnost ISSV (High-avaibility)
- Vysokou výkonnost ISSV (High-performance)
- Obnovu provozu ISSV (Disaster recovery)

Testy budou prokazovat plnění hodnot SLA, uvedených v kapitole Požadavky na provoz. Pro testování vysoké dostupnosti, výkonnosti a obnovy provozu vytvoří Poskytovatel samostatné testovací scénáře.

8.1.5. BEZPEČNOSTNÍ A PENETRAČNÍ TESTY

Objednatel v rámci testování ověří bezpečnost ISSV. Testy budou realizovány buďto Objednatelem nebo 3. stranou ve smluvním vztahu s Objednatelem. Penetrační testování bude v souladu s požadavky ZoKB, ISMS, penetrační testy budou realizovány vč. metodiky OWASP TOP10. Otestovány budou jak veřejná část ISSV, tak neveřejné části ISSV.

Realizátorovi penetračního testování bude poskytne Poskytovatel potřebnou součinnost – umožnění přístupu, přístup k datům, konzultace apod.

Výsledky penetračních testů jsou závazné a v případě nálezů je Poskytovatel povinen odstranit veškeré nálezy ve sjednaném čase dle smlouvy, neurčí-li Objednatel jinak. Testy budou mít v případě nálezů více iterací a Poskytovatel je povinen zajistit součinnost při všech penetračních testech.

8.2. NÁSTROJ PRO ŘÍZENÍ TESTOVÁNÍ

Poskytovatel v rámci dodání zajistí nástroj, v rámci kterého bude realizován sběr zjištění z testování (předpoklad service-desk nebo jiný specializovaný nástroj). Zjištění z testování budou klasifikovány podle závažnosti na minimálně tři stupně, bude možné Objednatelem a jeho testovacími týmy vkládat zjištění z testování do tohoto nástroje. Nástroj bude rovněž přístupný osobám, stanoveným Objednatelem.

Za hlášením zjištění z testováni bude existovat zpětná dohledatelnost řešení zjištění v čase a veškeré zjištění vč. jejich řešení bude možné předat Objednateli v strojově čitelném formátu.

8.3. TESTOVACÍ SCÉNÁŘE

Pro jednotlivé testy Poskytovatel nevrhne testovací scénáře, které budou předány Objednateli. Objednateli budou předány i testovací scénáře, které realizuje Poskytovatel.

Testovací scénář bude pokrývat oblast testování, pro každou funkcionalitu a proces bude existovat vlastní testovací scénář. Testovací scénáře mohou být sdružovány podle celků do větších souborů.

Testovací scénář bude vytvořen v českém jazyce a bude popisovat pokyny pro testovacího uživatele, vč. očekávaných výsledků operace. Scénář bude obsahovat i známé výjimky pro neautorizované operace, které budou rovněž testovány s výsledkem zamítnutí systémem.

9. POŽADOVANÉ LICENCE

9.1. LICENCE ISSV

Licence k ISSV, všem jeho částem, dokumentaci a zdrojovým kódům bude dodána jako výhradní licence pro Objednatele, přičemž licence bude reflektovat následující požadavky:

- Licence umožní užití Díla Objednatelem, jeho partnerům a veřejností
- Licence bude místně neomezená
- Licence bude početně neomezená
- Licence nebude omezovat užití ISSV, jeho modifikaci či rozvoj
- Licence bude neodvolatelná
- Licenci nebude mít nabyvatel povinnost využít
- Nabyvatel bude oprávněn udělovat sublicence
- Nabyvatel bude oprávněn postoupit licenci dalšímu subjektu

9.2. LICENCE PODPŮRNÉHO SW

ISSV bude vytvářen jako nové dodavatelské řešení. Bude-li pro jeho chod nezbytný podpůrný SW (v dokumentu rovněž uváděn jako Standardní SW), jehož není Poskytovatel vlastníkem, zajistí pro tento podpůrný SW Poskytovatel nevýhradní licenci, plnící veškeré práva v rozsahu nezbytném pro zajištění účelu ISSV.

9.3. LICENCE TECHNOLOGICKÉHO SW

Technologický SW (operační systém, databáze, virtualizace) zajistí Poskytovatel infrastruktury dle aktuálního katalogového listu SPCSS. V případě, že bude Poskytovatel potřebovat specifický technologický SW pro chod ISSV, musí zajistit licence ve stejném režimu jako licence podpůrného SW a požádat o výjimku Poskytovatele infrastruktury – Státní pokladnu Centrum sdílených služeb, s. p., pro nasazení v prostředí Poskytovatele infrastruktury. Pro tuto potřebu může Poskytovatel infrastruktury vyžadovat atestace, bezpečnostní protokoly a dokumentaci tohoto SW.

10. POŽADAVKY NA ŠKOLENÍ A DOKUMENTACI ISSV

10.1. POŽADOVANÁ ŠKOLENÍ

Poskytovatelem budou k ISSV v rámci dodání realizovaná školení pro Objednatele a další partnery Objednatele. Školení budou realizována v českém jazyce.

Školení budou kapacitně neomezená, realizovaná prezenčně v prostorách Objednatele a rovněž hybridně prostřednictvím telekonferenčního připojení dle výběru Objednatele. Školení proběhnou v termínech smluvených s Objednatelem. Každý typ školení bude realizován minimálně ve dvou termínech a každý termín bude mít minimální časovou alokaci 2 dny. Ze školení budou pořizované záznamy, které budou předány Objednateli.

Budou realizovaná následující školení:

- Školení testovacích uživatelů
- Školení koncových uživatelů
- Školení správců

Školení testovacích uživatelů bude realizováno před testování ISSV v testovacím prostředím. Školení bude korespondovat s testovacími scénáři. Cílem školení je předání informací o fungování ISSV, jeho UI a procesech vykonávaných v ISSV testerům, kteří by měli simulovat práci v ISSV dle popsaných rolí v rámci architektury.

Školení testovacích uživatelů by mělo být realizované pro uživatele Objednatele a jeho partnerů simulující jednotlivé role v systému. Součástí školení je i školení testerů simulujících chování občana v části ISSV pro přihlášené občany, tedy např. proces podání žádosti o změnu hlasovací místnosti a ostatní procesy realizované občany.

Školení koncových uživatelů po realizaci testování a nasazení ISSV do produkce bude realizováno Poskytovatelem pro uživatele Objednatele a jeho partnerů. Předmětem školení bude ovládání ISSV dle dané role koncového uživatele.

V rámci školení koncových uživatelů nebude realizované školení pro uživatele z řad voličů, petentů a kandidátů. Ti budou mít k dispozici školící materiály požadované níže v tomto dokumentu. Metodické vedení těchto koncových uživatelů zajistí Objednatel za případné vyžádané součinnosti Poskytovatele, viz. informace v kapitole Požadavky na řízení projektu poskytovatelem.

Školení správců bude realizovaná pro ICT pracovníky a věcné specialisty Objednatele či jiných technických správců Objednatele. Školení se bude zabývat správou a konfigurací jednotlivých modulů a funkcí, správu entit, služeb, číselníků, integrací, řešení nestandardních situací IS (identifikovaných jako možných Poskytovatelem v rámci procesů ISSV) a identifikace chybových kódů, pro vybrané správce bude součástí školení přístup k logům a zálohám, datová obnova, školení v oblasti zdrojových kódů, orientace v databázi a její správě, realizací rutin v ISSV a dohled automaticky spouštěných rutin.

Ve fázi metodické součinnosti po pilotním provozu (viz kapitola Požadavky na řízení fází a akceptační kritéria) **bude Poskytovatel spolupracovat s Objednatelem na školení dalších zapojených subjektů** státní správy. V rámci této součinnosti se Poskytovatel účastní metodických workshopů Objednatele pro partnerské subjekty a rovněž se bude podílet na školení editorů ISSV z řad partnerských subjektů. V rámci tohoto školení se předpokládá lektorská součinnost pro technickou oblast, ovládání funkcí ISSV, procesy ISSV a možné stavy během výkonu procesů.

Ve smlouvě jsou tato školení souhrnně uvedena jako „Školení“.

Školení mohou být předmětem připomínkování a v případě, že nebylo provedeno řádně a v souladu se smlouvou a touto dokumentací, musí takové školení dodavatel realizovat znovu s modifikacemi daného školení pro vypořádání připomínek, viz požadavky na školení a jejich akceptaci ve smlouvě.

10.2. POŽADOVANÁ DOKUMENTACE

Níže je uveden výčet požadované dokumentace, kterou Poskytovatel v rámci realizace Díla vytvoří. Dokumentace, které nemá charakter dokumentace řízení projektu, ale jedná se o dokumentaci související s ISSV, bude uložena on-premise v úložišti Objednatele. Tento požadavek se týká mj. veškeré systémové dokumentace, analytické dokumentace, testovacích protokolů, a především související bezpečnostní dokumentace.

10.2.1. ŠKOLÍCÍ DOKUMENTACE

Kromě realizovaných školení budou k dispozici:

- Uživatelské příručky – součástí systémové dokumentace, v editovatelné elektronické dokumentové podobě (.rtf,.docx,.doc) a rovněž jako dokumenty ve formátu PDF/A se strojově čitelnou textovou vrstvou. Příručky budou vytvořeny pro jednotlivé role v systému a zpřístupněny v rámci ISSV pro uživatele dle jejich role.
- FAQ –báze častých dotazů a odpovědí dostupná prostřednictvím UI ISSV

10.2.2. PŘEDIMPLEMENTAČNÍ ANALÝZA

V rámci analytické fáze projektu vytvoří Poskytovatel předimplementační analýzu. Předimplementační analýza bude popisovat Dílo do takového detailu, aby byla možná jeho realizace a zpracování Provozní dokumentace k ISSV Poskytovatelem. Předimplementační analýza je ve smlouvě vedena jako „Analýza“.

Předimplementační analýza musí obsahovat minimálně následující:

1. **Implementační část** – části za Objednatele doplní Objednatel a jeho zainteresované strany
    - Řízení projektu:
        - Administrativní údaje
        - Seznam kontaktních osob realizačního týmu (Poskytovatel, Objednatel, zainteresované strany Objednatele, techničtí správci Objednatele a další stanovení Objednatelem
        - Přístup do systému service-desk
        - Uvedení projektové metodiky a přístupu k řízení projektu Poskytovatelem
    - Popis průběhu implementace včetně podrobného harmonogramu implementace pro všechny části:
        - Podrobný harmonogram popisující všechny fáze implementace a milníky.
        - Plán kvalifikovaného seznámení Objednatele a jeho správců s dodaným dílem.
        - Plán implementace do jednotlivých prostředí
        - Předání do testovacího provozu – kontrola dodaného řešení Objednatelem před sepsáním akceptačního protokolu
        - Testovací provoz – kontrola dodaného řešení Objednatelem ve zkušebním provozu, který simuluje co nejvíce běžný provoz.
        - V rámci testovacího provozu požadovanou součinnost Objednatele
        - Uvedení do produkčního provozu a sepsání protokolu o předání a převzetí Díla.
    - Aktualizace business architektury
        - Bude revidovaná a aktualizovaná business architektura, na základě business architektury v technické specifikaci této zadávací dokumentace a bude

rozporcována do cílové podoby pro pokrytí procesů skrze konkrétní dodavatelské řešení ISSV

- Popis dodávaného řešení
  - bude popsáno cílové řešení ISSV, které bude vyvinuto Poskytovatelem, vč. cílové modularity – popis budou tvořit systémová a bezpečnostní část níže

2. **Systémová část:**
   - schéma a popis aplikační, systémové a síťové architektury a infrastruktury – topologie, vazby, funkční bloky, popis struktury adresářů a databáze, provázanost na údaje v ISZR, informace k infrastruktuře dohodnuté s Poskytovatelem infrastruktury Objednatele
   - Specifikace všech dodávaných SW prvků, konfigurace jak hlavních, tak i jejich významných dílčích částí, popis funkce v rámci dodaného řešení.
   - systémové požadavky pro běh ISSV,
   - popis prostředí a instancí ISSV
   - nastavení proti přetěžování systému,
   - popis aplikačních rozhraní pro možnosti aplikační, popř. procesní integrace
   - popis existujících vazeb a integrací
     - např. integrace na eSSL Objednatele, integrace na ISZR, NIA, JIP/KAAS, CAAIS, ISZR
   - podporované standardy při integraci systémů
     - datové, systémové, bezpečnostní apod.
   - možnosti zajištění rozšíření stávající funkcionality pro potřeby integrovatelnosti ISSV s okolními systémy – popis integrační platformy a způsobu integrace ISSV
   - seznam použitých technologií (např. ASP, PHP, XML, JavaScript, jQuery…)
   - režim správy ISSV (organizační matice, vč. uvedení správců a rozdělení kompetencí správy systému ISSV)
   - princip aktualizace
   - plány nasazování aktualizací, podle nichž budou průběžně vydávané záplaty testovány a následně aplikovány na IS
   - seznam licencí i open-source licencí a jejich parametry (licenční smlouvy budou následně dodány jako separátní dokumenty)

3. **Bezpečnostní část** – popis realizovaných bezpečnostních opatření, mechanismů a jejich návazností:
   - popis veškerých metod přístupů – systém, DB apod.
   - popis autorizace a autentizace uživatele
   - popis uživatelských rolí, jejich oprávnění
   - popis správy uživatelů
   - logování operací a chyb – výčet logů, akcí, jejich detailu, místa uložení
   - popis zálohování – výčet dat a SW částí, frekvence zálohování a umístění zálohy, princip obnovy, disaster recovery scenáře (ve spolupráci s Poskytovatelem infrastruktury Objednatele za infrastrukturu)
   - popis bezpečnostních opatření systému, vztah k jednotlivým rolím, k činnosti správce (např. doba timeout session, zasílání SMS při určitých akcích, omezení přístupu k logům apod.)
   - popis naplnění doporučení OWASP Top10 a NÚKIB, popis naplnění doporučení ISMS (ISO 27001)
   - popis naplnění ZoKB pro ISSV, informační systém veřejné správy v režimu kritické infrastruktury

- analýza rizik a informačních aktiv se zohledněním platných doporučení NÚKIB pro KII a posouzení varování NÚKIB pro ISSV s všechny komponenty (vč. Standardních SW)

Předimplementační analýza bude dodána jako editovatelný elektronický dokument, který bude obsahovat rovněž editovatelné přílohy – diagramy struktury DB a diagramy cílových architektur. Zmiňované diagramy v přílohách budou dodány v notaci Archimate ve výměnném formátu s příponou .xml a v případě diagramu struktury DB rovněž ve vybraném formátu pro zobrazení schématu DB. V případě, že formát bude vyžadovat specifický SW pro čtení, jímž Objednatel nedisponuje, bude poskytnut Objednateli Poskytovatelem na náklad Poskytovatele.

Akceptačním kritériem převzetí předimplementační analýzy bude obsažení výše požadovaných informací v takové podobě a detailu, aby bylo možné na základě těchto informací vytvořit cílový ISSV a nasadit jej do cílových prostředí a Objednatel v návrhu nevnímal nejasnosti. Zda návrh obsahuje nejasnosti ověří Objednatel v rámci připomínkovacího řízení, na nějž si vyhrazuje minimálně 14 kalendářních dní. Poskytovatel je následně povinen zapracovat připomínky do 7 kalendářních dní a předat novou verzi analýzy Objednateli k ověření vypořádání připomínek. Dobu připomínkování a zakomponování připomínek může Objednatel pozměnit v případě odůvodněného požadavku Poskytovatele.

10.2.3. SYSTÉMOVÁ DOKUMENTACE

Z předimplementační analýzy následně po změnách v průběhu vývoje a dodání ISSV bude vycházet systémová dokumentace, která bude zpracovaná dle požadavků zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů a zároveň bude obsahovat minimálně stejný rozsah informací a příloh jako předimplementační analýza.

Tato dokumentace bude součástí akceptace a Poskytovatel ji bude následně udržovat v aktuální podobě se zakomponováním aktualizací, rozvoje a změn ISSV do patřičné části systémové či bezpečnostní části, a to po dobu poskytování servisních služeb, tedy minimálně po dobu 5 let.

Dokumentace bude dodána jak v editovatelné elektronické dokumentové podobě (.rtf,.docx,.doc), tak jako soubory PDF/A se strojově čitelnou textovou vrstvou.

Kromě systémové dokumentace s reflexí požadavku zákona a rozdělením na bezpečnostní, systémovou část a část uživatelské příručky budou rovněž dodány dokumenty:

- dokumentace strategie obnovy,
- dokumentace skutečného provedení,
- dokumentace obsahující popis autorizačního konceptu a oprávnění,
- dokumentace obsahující zálohovací a archivační postupy,
- dokumentace obsahující instalační a konfigurační postupy,
- dokumentace obsahující bezpečností nastavení související s ISSV

Poskytovatelem bude dále zpracována následující dokumentace dle požadavků Systému řízení bezpečnosti informací Objednatele. Dokumentace bude zpracována v šablonách Objednatele, které budou Poskytovateli poskytnuty. Bude se jednat o následující dokumenty:

- Bezpečnostní politika pro ISSV
- Plán zvládání rizik
- Prohlášení o aplikovatelnosti
- Plán kontinuity činností
- Zpráva o hodnocení aktiv a rizik

Veškerá dokumentace k ISSV bude psaná v českém jazyce.

10.3. DODÁNÍ ZDROJOVÝCH KÓDŮ

Poskytovatel v rámci dodání dodá zdrojové kódy celého ISSV a jeho modularity v editovatelné elektronické dokumentové podobě a zároveň budou vloženy do nástroje GIT či jiného nástroje Objednatele.

Ke zdrojovým kódům bude dodána dokumentace popisující strukturu zdrojových kódů, jejich syntaxi, provázanost kódů, způsob jejich nasazení a spuštění. Ke zdrojovým kódům a jejich praktickému využití bude realizováno školení Poskytovatele, viz. kapitola Požadovaná školení.

Požadovány jsou v rámci zdrojových kódů a jejich dokumentace mimo jiné databázové modely, popis vytvoření Software ze zdrojové formy, vysvětlení obsahu jednotlivých programových modulů a jejich klíčových funkcí ve formě komentářů ve Zdrojových kódech, a to nejméně v kvalitě obvyklé pro opensource projekty.

V případě změn systému v rámci provozní fáze (během poskytování servisních prací) budou zdrojové kódy aktualizované při vydání nové verze ISSV po jejím otestování a přijetí do provozu. Zdrojové kódy budou verzované a pro každý release verze ISSV budou k dispozici odpovídající zdrojové kódy.

11. POŽADAVKY NA PROVOZNÍ PODPORU

Kapitola popisuje provozní podporu Poskytovatele, která bude poskytována na základě uzavřené servisní smlouvy. V případě, že nebude uzavřena servisní smlouva, bude Poskytovatelem poskytnuta dvouletá záruka na jakost, funkčnost a dostupnost ISSV, jeho komponent a jakost souvisejících výstupů projektu v rozsahu daném smlouvou ode dne akceptace výstupu projektu.

11.1. POŽADOVANÉ SERVISNÍ SLUŽBY A JEJICH ROZSAH

Poskytovatelem bude k ISSV poskytnuta servisní podpora (paušální služby) spočívající se v zajištění rutinního bezchybného fungování ISSV, zajištění legislativní aktuálnosti ISSV, zajištění bezpečnosti ISSV, zajištění součinnosti s Objednatelem a jeho partnery, návrhů optimalizace a zajištění fungování a zalicencování Standardního SW, je-li součástí dodání.

Požadavky na fakturaci, akceptaci plnění a procesy v rámci poskytování servisních služeb jsou detailně stanoveny v rámci servisní smlouvy a pro Poskytovatele jsou závazné. Požadavky na výkazy jsou popsány níže v tomto dokumentu.

Poskytovatel pro zajištění tohoto cíle bude realizovat následující servisní činnosti:

- provozování service-desku Poskytovatele
- udržování aktuální Dokumentace ISSV
- lokalizace a odstraňování Incidentů a provádění Servisních zásahů
- zajištění dostupnosti a funkčnosti ISSV
- podávání pravidelných Výkazů (např. plnění SLA Paušálních služeb, kvantifikace Žádostí, vytíženost ISSV a další)
- maintenance a úpravy ISSV, včetně zajištění, implementace a instalace Aktualizací, patchů anebo jiných updatů ISSV
- sledování souladu ISSV s obecně závaznými právními předpisy a informování Objednatele o případném nesouladu ISSV s obecně závaznými právními předpisy a udělovat v tomto směru Objednateli odborné rady k dosažení souladu ISSV s legislativou
- Aktualizace ISSV z důvodu legislativních změn (do 10člh/měsíc)
- Aktualizace ISSV z důvodu bezpečnosti
- Řešení bezpečnostních incidentů
- Pravidelná profylaxe ISSV
- Pravidelné testování, vč. součinnosti při penetračním testování nebo auditu kybernetické bezpečnosti
- Pravidelné ohodnocení rizik a informačních bezpečnosti
- návrhy optimalizace ISSV, databází, komunikačních nastavení a dalších komponent technického řešení ISSV
- poskytnutí součinnosti při realizaci schválených optimalizací
- podpora a správa Standardního software sestávající z řešení Incidentů spojených s provozem Standardního software (je-li takový Standardního software součástí ISSV), vč. bezpečnostních aktualizací a podpory výrobce SW
- udržování Nevýhradní licence k Standardnímu software v rozsahu a za podmínek dle smlouvy, a to po celou dobu trvání smlouvy
- zajištění a udržování maintenance Standardního software, instalace, implementace a integrace aktualizací Standardního software a poskytnutí podpory (subscription / license maintenance) Standardnímu software, včetně nejnovějších verzí tohoto Standardního software Objednateli

a dalších souvisejících služeb v souladu s jeho standardními obchodními podmínkami, na dobu do skončení doby trvání této smlouvy

- komunikace s třetími osobami provozujícími či poskytujícími služby údržby informačním systémům napojeným na ISSV, které nejsou Poddodavateli, v rozsahu dle potřeb Objednatele
- Spolupráce s Poskytovatelem infrastruktury při řešení požadavků Objednatele, při zajišťování maintenance či při řešení zjištění/incidentu

Všechny aktivity vyjma analýzy rozvojových požadavků a realizace rozvoje dle požadavku Objednatele budou řešeny v rámci paušální servisní podpory. Realizace rozvoje bude řešena na základě rámcové smlouvy a konkrétních objednávek rozvoje Objednatele.

Poskytovatelem budou vyhodnocovány změny legislativy a rovněž aktuální bezpečnostní situace a varování v oblasti kyberbezpečnosti od bezpečnostních složek, NÚKIB, poskytovatelů antivirových řešení apod., vůči těmto zjištěním bude komparovat nastavení ISSV a v případě, že identifikuje potenciální zranitelnost ISSV nebo nutnost změn s ohledem na legislativu, bude o tomto informovat Objednatele a následně provede vytvoření aktualizace/opravy, kterou nasadí dle procesu nasazování aktualizací.

V případě legislativních aktualizací platí, že legislativní aktualizace menšího rozsahu (do 10člh/měsíc včetně) jsou řešeny v rámci paušálních servisních služeb. V případě, že se jedná o aktualizaci většího rozsahu (nad 10člh/měsíc), bude takováto aktualizace předmětem rozvojových služeb Poskytovatele.

Pokud o změně/zjištění bude informován nejprve Objednatel či Poskytovatel infrastruktury Objednatele, oznámí jej Poskytovateli dle procesu hlášení zjištění.

V případě, že bude Objednatelem zjištěna chyba systému, zranitelnosti nebo došlo k bezpečnostnímu incidentu, bude o tomto informovat Poskytovatele v souladu s procesem uvedeným v tomto dokumentu a nahlásí událost prostřednictvím service-desk, který po dobu servisní podpory bude provozovat Poskytovatel.

Poskytovatel bude v rámci nastavené smlouvy kvartálně realizovat profylaxi ISSV, v rámci které ověří jeho stav, parametry a vyhodnotí nutnost změn. V případě, že se bude jednat o funkční vady, které ohrožují funkčnost, bezpečnost ISSV, případně dochází k nesouladu s legislativou, provede opravy po schválení Objednatelem dle SLA a nasadí je po odsouhlasení Objednatele.

Součástí služeb bude pravidelné roční testování ISSV v rozsahu testů definovaných v kapitole Požadavky na testování. Výčet může být zúžen Objednatelem. Testování bude rovněž probíhat při změnách ISSV a nasazování nových verzí/aktualizací. I pro tyto testy platí, že v případě nálezů vad bude test víceiteranční do vyhodnocení bez nálezů. Součástí ročního otestování bude ověření, že ISSV (a všechny jeho funkcionality vč. Standardního SW) jsou dostupné pro přístup on-premise v síti CMS 2.0. i při nedostupnosti veřejné sítě internet.

Součástí služeb bude součinnost při realizaci ročního penetračního testování ISSV Objednatelem nebo třetí stranou, zajištěnou Objednatelem, při které Poskytovatele poskytne vyžádanou součinnost Objednateli a dalším třetím stranám zajištěným Objednatelem – umožnění přístupu, přístup k datům, konzultace apod. Penetrační testy budou splňovat stejné podmínky jako penetrační testování při vytváření ISSV, definované touto technickou specifikací. Stejný požadavek na součinnost platí v případě auditu kybernetické bezpečnosti, který bude Objednatel nebo třetí strana vykonávat.

Poskytovatel bude rovněž v oblasti bezpečnosti spolupracovat s Objednatelem a jeho Poskytovatelem infrastruktury na pravidelném ročním hodnocení kybernetických rizik a hodnocení aktiv.

Poskytovatel rovněž poskytne proaktivní součinnost v případě potřeby optimalizace ISSV, jeho komponent nebo databáze a stejnou součinnost poskytne v případě, že třetí strana bude realizovat optimalizace s dopadem na ISSV.

Je-li součástí dodání ISSV Standardní SW (tedy SW Poskytovatele nebo třetí strany dostupný na trhu s udělením nevýhradní licence), musí k tomuto SW Poskytovatel zajistit stejnou podporu jako k ISSV, tedy musí zajistit jeho aktuálnost, bezpečnost, dostupnost, reakční schopnost v souladu s SLA, zajištění souladu s legislativou, řešení incidentů a jiných hlášení Objednatele a jeho partnerů. Navíc musí poskytovatel zajistit platnou licenci Standardního SW po dobu poskytování servisních služeb.

11.2. ROZVOJOVÉ SLUŽBY

Rozvojové služby budou poskytovány na rámcovou smlouvu na bázi objednávek v režimu pevná sazba a termín nebo pevná cena a vykázaný čas, blíže specifikovaných servisní smlouvou.

Rozvoj bude pokrývat požadované rozšíření funkcionalit ISSV, změny struktury databáze, rozšíření existujících integrací a vytváření nových elektronických formulářů, vč. jejich napojení na databázi ISSV, případně další rozvojové aktivity v oblasti informačního systému a souvisejícího SW. Pokud je uvedené důsledkem zjištění v oblasti bezpečnosti nebo chybou systému, nejedná se o rozvoj, ale o činnost řešenou Poskytovatelem v rámci servisní podpory. Součástí rozvojových služeb poskytovaných na rámcovou smlouvu budou rovněž školení Poskytovatele dle požadavků Objednatele, případně služby součinnosti v rámci exit-plánu.

Požadavky na nabídku, uzavírání dílčích smluv a objednávek, fakturaci, akceptaci plnění a procesy v rámci rozvoje jsou detailně stanoveny v rámci servisní smlouvy a pro Poskytovatele jsou závazné. Požadavky na výkazy jsou popsány níže v tomto dokumentu.

Požadované rozvojové služby jsou následující:

- Rozvoj ISSV, jeho funkcionalit a datového obsahu
- Vytváření a úpravy elektronických formulářů, jejich konfigurace a napojení jejich atributů na databázi ISSV
- Jakékoli služby nad rámec paušálních služeb vyžadované Objednatelem
- Školení dle požadavků Objednatele, konzultační služby, reporting a jednorázové analýzy nad rámec paušálních služeb;
- Aktualizace ISSV způsobené změnami příslušných obecně závazných právních předpisů (legislativní update) – nad 10člh pracnosti;
- Komunikace s třetími osobami provozujícími či poskytujícími služby údržby informačním systémům napojeným na ISSV (integrace), které nejsou poddodavateli, v rozsahu dle potřeb Objednatele **nad rámec paušálních služeb**
- Rozvojová spolupráce s Poskytovatelem infrastruktury na vyžádání Objednatele (**spolupráce nad rámec paušálních služeb)**
- Součinnost v rámci exit-plánu (blíže definováno smlouvou)

11.3. SLA SERVISNÍCH SLUŽEB

V rámci SLA servisních služeb budou služby poskytovány dle období. Období provozu ISSV jsou následující:

- Období rutinního chodu ISSV,
- Období přípravy celostátních voleb a
- Období celostátních voleb.

Období rutinního chodu ISSV je období, kdy nedochází k celostátním volbám a systém je využit pro volby menšího rozsahu nebo pro vyhodnocení minulých voleb, pro školení uživatelů a testování ISSV či jiných mimovolebních provozních aktivit.

Období přípravy celostátních voleb a Období celostátních voleb jsou z pohledu SLA obdobím, pro které platí vyšší hodnoty SLA, jelikož se jedná o období, kdy ISSV plní svou funkci procesního pokrytí přípravy a realizace voleb a musí být neustále dostupný a funkční. Období přípravy celostátních voleb je stanoveno od oficiálního vyhlášení voleb, tedy nejpozději 3 měsíce před Obdobím celostátních voleb.

Období celostátních voleb platí pro následující volby:

- Volby do Poslanecké sněmovny
- Volby do Senátu (vč. doplňovacích a opakovaných voleb)
- Volby do zastupitelstev krajů (vč. „mimořádných“ voleb)
- Volby do zastupitelstev obcí a měst (kromě „mimořádných“ voleb)
- Volba prezidenta republiky
- Volby do Evropského parlamentu

Předpokládané rozdělení období pro poskytování servisních služeb Poskytovatelem bude dodáno Objednatelem pro následující rok v rámci tzv. volebního kalendáře pro umožnění alokace kapacit Poskytovatele pro plnění SLA.

Objednatel nedokáže ovlivnit a predikovat konání celostátních voleb v mimořádných termínech. I pro tyto stavy nicméně musí být provoz ISSV Poskytovatelem zajištěn v režimu Období přípravy celostátních voleb a Období celostátních voleb – nevztahuje se na „mimořádné“ volby do zastupitelstev obcí a měst. Objednatel se pro tyto stavy zavazuje informovat Poskytovatele o mimořádných volbách nebo změně harmonogramu voleb neprodleně po obdržení potvrzené informace o jejich konání.

Níže jsou uvedeny SLA pro jednotlivá období. Do doby dostupnosti systému se nezapočítávají aktualizace a opravy ISSV, které jsou Poskytovatelem v souladu se Servisní smlouvou realizovány mimo pracovní dobu (8-17h).

Pro odstranění bezpečnostního incidentu kategorie II či III je možné udělit výjimku Objednatelem a realizovat změnu po schválení Objednatele i v pracovní době, bez dotčení SLA garantované dostupnosti ISSV.

Společná SLA:

Režim provozu ISSV je 24 x 7

Režim podpory provozu Poskytovatelem je 24 x 7

11.3.1. Garantovaná dostupnost ISSV

Poskytovatel je povinen zabezpečit Dostupnost ISSV minimálně v hodnotách uvedených v tabulce níže:

Č.	Provozní parametr	Hodnota parametru	Popis smluvní sankce (pokuty)	Výše smluvní pokuty v Kč

1.	Režim provozu ISSV a podpory (tj. poskytování Služeb)	24/7 (non-stop)	Nedefinováno.	Nedefinováno
2.	Dostupnost ISSV (Rutinní provoz)	99,5 % za měsíc	Za každou započatou jednu desetinu procenta nedodržení Dostupnosti ISSV.	Dvě procenta (2 %) z Ceny paušálních služeb za každou započatou jednu desetinu procenta (0,1 %) nedodržení Dostupnosti Systému.
3.	Dostupnost ISSV (Období přípravy celostátních voleb a období celostátních voleb)	99,9 % za měsíc	Za každou započatou jednu desetinu procenta nedodržení Dostupnosti ISSV.	Dvě procenta (2 %) z Ceny paušálních služeb za každou započatou jednu desetinu procenta (0,1 %) nedodržení Dostupnosti Systému.
4.	Stanovená doba měření Dostupnosti ISSV	24/7 (non-stop)	Nedefinováno.	Nedefinováno

„**Rutinní provoz**“ znamená v období, kdy nedochází k žádným volbám, referendům a ISSV je využit pro vyhodnocení minulých voleb nebo pro školení uživatelů a testování ISSV – viz popis výše;

„**Období přípravy celostátních voleb a období celostátních voleb**“ znamená období, kdy ISSV plní svou funkci procesního pokrytí přípravy a realizace celostátních voleb. – viz popis výše.

Výpočet Dostupnosti ISSV

Pro výpočet dostupnosti ISSV se použije následující vzorec:

Dostupnost ISSV v % = [(Td – Tn) / Td] * 100

- **Td** – znamená dobu, po kterou měl být Systém dostupný podle výše uvedené Dostupnosti ISSV (uvedené v tabulce výše) po odečtení dob, které se dle tohoto dokumentu nepovažují za nedostupnost ISSV;
- **Tn** – znamená dobu, kdy Systém byla v rozporu s touto Přílohou č. 1 nedostupný;
- **Doby Td a Tn** se počítají na celé minuty. Dostupnost ISSV se vyjadřuje procentní hodnotou zaokrouhlenou na dvě desetinná místa.

Za nedostupnost ISSV se podle dohody Stran nepovažují doby nedostupnosti způsobené:

- prováděním Plánovaných odstávek ISSV v souladu s následující subkapitolou
- mimořádnou nepředvídatelnou a nepřekonatelnou překážkou vzniklou nezávisle na vůli Poskytovatele,
- prodlením Objednatele anebo jiným důvodem, který prokazatelně zavinil Objednatel;
- provedením Servisních zásahů či jiných činností objednaných či vyžadovaných Objednatelem na základě smlouvy, pokud Poskytovatel Objednatele na nedostupnost ISSV předem upozornil a Objednatel s touto skutečností výslovně souhlasil.

Poskytovatel je povinen obnovit Dostupnost ISSV v maximální době pro obnovení Dostupnosti ISSV uvedené ve výše uvedené tabulce.

11.3.2. Plánované odstávky ISSV

Poskytovatel je oprávněn provést Plánovanou odstávku ISSV jen za podmínek stanovených v tomto bodu, jinak se doba jejich trvání považuje za dobu nedostupnosti ISSV. Poskytovatel je povinen ohlásit Plánovanou odstávku ISSV alespoň pět (5) dnů předem Kontaktní osobě Objednatele pro věcné plnění smlouvy.

Nedohodnou-li se Strany jinak, je Poskytovatel oprávněn provést Plánovanou odstávku ISSV pouze za účelem instalace nových verzí aplikačního a systémového programového vybavení ISSV nebo provedení profylaktických prohlídek ISSV, a jedině v časovém intervalu („**Servisní okno**“) každý čtvrtek v době od 18:00 do 07:00 následujícího dne.

V případě, že bude Plánovaná odstávka trvat déle než jednu (1) hodinu, oznámí je Poskytovatel písemně Kontaktní osobě Objednatele pro věcné plnění minimálně tři (3) dny předem. Kontaktní osoba Objednatele tuto odstávku potvrdí písemně Poskytovateli. Plánované odstávky ISSV budou plánovány výhradně mimo dobu požadované Dostupnosti ISSV, tedy mimo měřený úsek, existuje-li taková doba. Plánované odstávky ISSV trvající méně než jednu (1) hodinu je možné dohodnout telefonicky minimálně čtyři (4) hodiny předem.

Poskytovatel je oprávněn v jednom (1) měsíci využít pouze čtyři (4) Servisní okna. Poskytovatel využívá Servisní okna pouze tehdy, pokud příslušné údržbové činnosti či jiné Servisní zásahy nelze provést bez omezení Dostupnosti ISSV. Servisní okna, která Poskytovatel v příslušném měsíci nevyužil, se do dalšího měsíce nepřevádějí; Poskytovateli za nevyužitá Servisní okna nevzniká žádné právo na jakékoliv plnění.

Objednatel je oprávněn určit pro provedení ohlášené Plánované odstávky ISSV jinou dobu jejího provedení, než je doba Servisního okna, pokud by nedostupnost ISSV spojená s využitím Servisního okna mohla Objednateli nebo jiné osobě způsobit škodu či újmu; v takovém případě se Objednatelem určená doba pro provedení Plánované odstávky ISSV započítává na to Servisní okno, jehož využití Poskytovatel původně ohlásil.

Objednatel poskytne po předchozí dohodě Poskytovateli přístup do svých prostor nebo k technickým prostředkům, je-li takový přístup nezbytný k provedení Plánované odstávky ISSV nebo jiných servisních činností Poskytovatelem.

11.3.3. Kategorizace incidentů, reakční doba a doba vyřešení, sankce

Při realizaci plnění předmětu této smlouvy a zejména při poskytování Paušálních služeb může dojít k Incidentům, které jsou hlášeny na service-desk. Incidenty jsou rozděleny do následující klasifikace:

- **Kategorie III** – Incident, který má zásadní a negativní dopad na Systém, nebo znemožňující či významně omezující užívání Systému; např. způsobuje „zamrznutí“ anebo „zhroucení“ během normálního používání, způsobuje ztrátu anebo porušení dat během běžného užívání Systému a způsobuje, že Systém je nefunkční. Za Incident v této kategorii se považuje i kybernetický bezpečnostní incident kategorie II či III dle § 31 odst. 2 VKB.
- **Kategorie II** – Incident omezující užívání Systému, tj. způsobuje významné problémy při používání, avšak umožňující provoz základních funkcí Systému nebo způsobuje, že část dodaného Systému se významně odchyluje od specifikace v Dokumentaci, avšak neomezuje významně jeho funkčnost. Do této kategorie patří i nemožnost přístupu k Systému pouze pro některé uživatele. Za Incident v této kategorii se považuje i kybernetický bezpečnostní incident kategorie I dle § 31 odst. 2 VKB KIB, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv.

- **Kategorie I** – Incident, který se vyskytuje v části Systému, komplikuje postupy při práci se Systémem a nemá vliv na ostatní funkce. Incident se může projevovat v neshodě ovládání či výstupů s chováním popsaným v Dokumentaci. Za Incident v této kategorii se považuje i jakýkoliv Incident, který nespadá ani do jedné z výše uvedených kategorií (např. špatná grafická úprava aplikace, špatný pravopis u nápovědy apod.) anebo interní kybernetický bezpečnostní incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv.

Incidenty budou řešeny dle následujících SLA podle příslušného období:

Rutinní provoz

Kategorie Incidentu	Reakční doba	Doba vyřešení
	Uvedené doby se počítají 24/7	
III	4 hodiny	8 hodin
II	4 hodiny	24 hodin
I	4 hodiny	4 dny

Období přípravy celostátních voleb a období celostátních voleb

Kategorie Incidentu	Reakční doba	Doba vyřešení
	Uvedené doby se počítají 24/7	
III	1 hodina	4 hodiny
II	2 hodiny	8 hodin
I	4 hodiny	24 hodin

Zjištění a incidenty se prioritizací dle kategorie Incidentu, kdy kategorie I má nejnižší prioritu a řeší se až po kategoriích III a II. Pro odstranění Incidentu kategorie II či III můžou platit výjimečná pravidla. Takovýto Incident s potřebou okamžitého řešení (v Období přípravy voleb nebo voleb) může nahlásit oprávněná osoba Objednatele. V tomto případě Poskytovatel prověří operativně **situaci do jedné (1) hodiny a bude informovat Objednatele o výsledku prověření hlášení**. V případě, že bude Incident potvrzen, bude Poskytovatelem zavedeno do service-desk jako požadavek kategorie III s přiřazením odpovědné osoby a řešením v rámci SLA.

Poruší-li Poskytovatel svoji povinnost zabezpečit Dostupnost Systému minimálně v hodnotě uvedené v tomto dokumentu, je Objednatel oprávněn požadovat po Poskytovateli slevu z Ceny paušálních služeb za příslušný měsíc ve výši dvě procenta (2 %) z Ceny paušálních služeb za každou započatou jednu desetinu procenta (0,1 %) nedodržení Dostupnosti Systému.

Poruší-li Poskytovatel svoji povinnost dodržet sjednanou Reakční dobu, je Objednatel oprávněn požadovat (v každém jednotlivém případě) po Poskytovateli zaplacení smluvní pokuty ve výši:

Rutinní provoz

5.000 Kč (slovy: pět tisíc korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie III;

3.000 Kč (slovy: tři tisíce korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie II;

1.000 Kč (slovy: jeden tisíc korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie I;

Období přípravy voleb a období voleb

10.000 Kč (slovy: deset tisíc korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie III;

6.000 Kč (slovy: šest tisíc korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie II;

2.000 Kč (slovy: dva tisíce korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie I.

Poruší-li Poskytovatel svoji povinnost dodržet sjednanou Dobu vyřešení, je Objednatel oprávněn požadovat (v každém jednotlivém případě) po Poskytovateli zaplacení smluvní pokuty ve výši:

Rutinní provoz

8.000 Kč (slovy: osm tisíc korun českých) za každou započatou hodinu prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu Kategorie III;

4.000 Kč (slovy: čtyři tisíce korun českých) za započatou hodinu prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu Kategorie II;

1.000 Kč (slovy: jeden tisíc korun českých) za každý započatý den prodlení nad rámec sjednané Doby vyřešení v případě každého Incidentu Kategorie I;

Období přípravy voleb a období voleb

16.000 Kč (slovy: šestnáct tisíc korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie III;

8.000 Kč (slovy: osm tisíc korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie II;

2.000 Kč (slovy: dva tisíce korun českých) za každou započatou hodinu prodlení nad rámec sjednané Reakční doby v případě Incidentu dle Kategorie I.

11.4. NAHLAŠOVÁNÍ ZJIŠTĚNÍ/INCIDENTŮ A NASAZOVÁNÍ AKTUALIZACÍ

Nahlašování zjištění a incidentů bude realizované Objednatelem do systému service-desk, který Poskytovatel zřídil v rámci realizace projektu a bude dále využit v rámci servisní podpory. Do systému service-desk bude umožněn přístup vybraným pracovníkům, kteří budou vedeni jako oprávněné osoby k nahlášení zjištění či incidentů. Alternativně lze zjištění/incident nahlásit prostřednictvím hot-line nebo e-mailem na adresu definovanou jako součást service-desk.

Popis incidentu/zjištění bude minimálně následujícího rozsahu:

- krátký a rámcově výstižný název Incidentu;
- identifikace části Systému, kterých se Incident týká;
- určení prostředí, v němž k Incidentu došlo anebo které je Incidentem zasaženo;
- detailní popis Incidentu, průvodních jevů a všech významných souvisejících informací;
- kategorii Incidentu (I., II., III.); a
- identifikaci oprávněné osoby včetně její lokality (pracoviště).

V případě, že některá z náležitostí výše chybí anebo je nedostatečná, může si Poskytovatel vyžádat její doplnění od ohlašovatele; tato skutečnost však nemá vliv na určení času nahlášení incidentu, avšak v případě oprávněné žádosti o doplnění se doba vyřešení přerušuje okamžikem doručení žádosti o doplnění a běží dále od okamžiku řádného doplnění dle žádosti.

Čas nahlášení se dle komunikačního kanálu určuje následovně:

- zadáním Incidentu do service-desku, pak se za Čas nahlášení incidentu považuje čas vytvoření ticketu v service-desku;
- písemně na e-mailovou adresu, pak se za Čas nahlášení incidentu považuje čas odeslání e-mailu z e-mailového serveru ohlašovatele, nebo
- telefonicky čas ukončení telefonického hovoru.

Poskytovatel je povinen prokazatelným způsobem bezodkladně potvrdit přijetí hlášení o Incidentu, a to vždy prostřednictvím service-desk a dodržet požadovanou reakční dobu vyplývající z kategorizace příslušného incidentu. Nepotvrdí-li Poskytovatel přijetí Incidentu, nemá to vliv na čas nahlášení incidentu.

Zjištění a incidenty se prioritizací dle kategorie zjištění/incidentu, kategorie I má nejnižší prioritu a řeší se až po kategoriích III a II. Čas vyřešení může být prodloužen v případě, že:

- došlo k zásahu vyšší moci,
- vyskytly se překážky na straně Objednatele, jeho Poskytovatele infrastruktury nebo třetích stran, znemožňující řádné poskytování služeb
- bylo řešení incidentu přerušeno z písemného pokynu Objednatele

Všechny zjištění a incidenty budou hlášeny oprávněnými osobami k nahlášení zjištění či incidentů. Součástí hlášení bude popis závady či bezpečnostního incidentu, klasifikace požadavku dle uvedených kategorií, uvedení funkcionality/komponenty/služby, případně screenshot nebo jiný důkaz hlášení.

Poskytovatel hlášení převezme a bude informovat o přijetí požadavku. Následně vzdáleným přístupem provede analýzu nahlášeného. Pro tuto potřebu mu bude umožněn vzdálený přístup Poskytovatelem infrastruktury prostředí.

Po analýze bude Poskytovatel informovat Objednatele o možných dopadech realizace změn, rozsahu změn, pravděpodobném čase odstranění nefunkčnosti a případně alternativních způsobech řešení

(takové řešení musí být následně schváleno Objednatelem) a po odstranění závady, vyřešení incidentu bude informovat Objednatele o:

- vyřešení problému přímo v rámci prostředí
- možnosti nasazení aktualizačního balíčku v případě většího množství závad

Odstranění vad bude nejprve provedeno v testovacím prostředí v případě, že se vada projevuje v obou prostředích. Nasazení aktualizačního balíčku bude realizováno nejprve do testovacího prostředí.

Pro odstranění bezpečnostního incidentu kategorie II či III můžou platit výjimečná pravidla. Takovýto incident s potřebou okamžitého řešení (v období přípravy voleb nebo voleb) může nahlásit oprávněná osoba Objednatele i telefonicky s uvedením urgentnosti. V tomto případě Poskytovatel prověří operativně situaci do 1 hodiny a bude informovat Objednatele o výsledku prověření hlášení. V případě, že bude hlášení potvrzeno, bude Poskytovatelem zavedeno do service-desk jako požadavek kategorie III s přiřazením odpovědné osoby a řešením v rámci SLA.

Incidenty budou Objednatelem rovněž hlášeny Poskytovateli infrastruktury Objednatele. V případě, že nebude jednoznačně možné určit odpovědnost za řešení incidentu/zjištění, bude nezbytná součinnost Poskytovatele a Poskytovatele infrastruktury. Pro tuto potřebu bude stanoven proces po jednání mezi subjekty (viz kapitola Požadavky na řízení fází a akceptační kritéria).

Poskytovatel je v tomto procesu povinen poskytnout Poskytovateli infrastruktury Objednatele součinnosti při analýze, nalezení chyby a následném řešení v případě sdílení odpovědnosti.

Odpovědnosti řešení incidentů/zjištění jsou následující:

- Dostupnost infrastruktury, operačního systému, databázového serveru – **Poskytovatel infrastruktury**
- Dostupnost ISSV, dostupnost databáze – Poskytovatel
- Monitoring služeb infrastruktury – **Poskytovatel infrastruktury**
- Logování – **Poskytovatel infrastruktury (SIEM)/Poskytovatel (ISSV)**
- Odezva ISSV – **Poskytovatel infrastruktury (infrastruktura)/Poskytovatel (ISSV)**
- Aplikační chyba ISSV – **Poskytovatel**
- Bezpečnostní zranitelnost kódů ISSV – **Poskytovatel**
- Bezpečnostní zranitelnost infrastruktury, operačního systému, databázového serveru – **Poskytovatel infrastruktury**
- Zálohování a obnova – **Poskytovatel infrastruktury (zálohovací infrastruktura, DB server) /Poskytovatel (ISSV)**
- Chyba komunikace ISSV – **Poskytovatel/3.strana (vlastník integrované aplikace)**

11.5. ŽIVOTNÍ CYKLUS INCIDENTU

Po zadání požadavku na řešení incidentu se požadavek ohlašovatele zanese do service-desku, který si po dobu řešení nese základní informace, v jakém stavu se požadavek nachází. Všechny stavy požadavku budou notifikovány. Pro řešení Incidentů jsou definovány následující stavy:

- **Požadavek zadán,**
- **Požadavek přiřazen,**
- **Požadavek v řešení,**

- **Požadavek v čekání,**
- **Požadavek vyřešen,**
- **Požadavek ověřen,**
- **Požadavek uzavřen.**

Význam stavů požadavku:

- Požadavek **zadán** (NEW) – znamená, že požadavek ohlašovatele byl zadán do service-desku.
- Požadavek **přiřazen** (ASSIGNED) – znamená, že požadavek byl přiřazen odpovědné osobě na straně Poskytovatele, která tento požadavek bude řešit.
- Požadavek **v řešení** (SOLUTION) – znamená, že požadavek začal řešit přiřazený řešitel. Označením požadavku v řešení (SOLUTION) končí Reakční doba.
- Požadavek **v čekání** – zde jsou dvě varianty, proč požadavek může být v tomto stavu:
  - čeká na vyjádření ohlašovatele,
  - čeká na dodávku třetí strany.
- Požadavek **vyřešen** – znamená, že požadavek byl důkladně analyzován Poskytovatelem a požadavek:
  - byl zpracován a vyřešen trvale (FIXED) – požadavek byl Poskytovatelem shledán jako oprávněný a byly učiněny kroky vedoucí k odstranění příčiny nahlášeného Incidentu Poskytovatelem, které nezpůsobí vedlejší nežádoucí efekty v podobě zhoršení jiných funkcionalit ISSV;
  - byl zamítnut (INVALID) – požadavek byl Poskytovatelem shledán jako neoprávněný, nejedná se o Incident nebo chybu způsobenou stranou Poskytovatele;
  - nebude zapracován (WONTFIX) – požadavek byl při analýze Poskytovatelem shledán jako oprávněný, avšak po domluvě s Objednatelem bylo rozhodnuto o jeho nezapracování, tj. řešení Incidentu neprováděním dalších činností;
  - je označen jako duplikát (DUPLICATE) – požadavek byl analyzován Poskytovatelem a prohlášen jako duplikát jiného požadavku, který byl stranou ohlašovatele položen. Při označení duplicitního požadavku se budou Strany navzájem informovat, tj. Incident nebude řešen;
  - nepodařilo se analyzovat nebo se nepodařilo nasimulovat na straně Poskytovatele (WORKSFORME) Incident. V tomto případě bude požadavek dál diskutován a analyzován Poskytovatelem;
  - může se ze stavu vyřešen vždy přesunout do stavu v řešení (SOLUTION) v případě, kdy strana ohlašovatele nesouhlasí s řešením ze strany Poskytovatele (REOPEN).
- Požadavek **ověřen** (VERIFIED) – znamená, že Řešení požadavku bylo potvrzeno ze strany ohlašovatele, včetně funkčnosti a bezpečnosti navrhovaného Řešení. Potvrzením požadavku (VERIFIED) končí doba trvání Incidentu a Doba vyřešení incidentu.
- Požadavek **uzavřen** (CLOSED) – znamená, že řízení ohledně požadavku bylo ukončeno a Řešení požadavku bylo potvrzeno Objednatelem.

11.6. VÝKAZ A REPORT

Výkaz vždy ve vztahu k **Paušálním službám** bude obsahovat:

Přehled:

- počet řešených a doposud nevyřešených Incidentů a jejich kategorii;
- počet Incidentů a jejich kategorii vyřešených za měsíc, za který je Výkaz vyhotovován;

- počet jiných požadavků pověřených uživatelů;
- počet Servisních zásahů k jednotlivým Incidentům;
- výše smluvních pokut, na které vzniklo Objednateli právo za daný měsíc (dle servisní smlouvy i tohoto dokumentu)

Podrobná část:

- seznam Incidentů a vad s uvedením jejich stručného popisu;
- kompletní záznam o Úkonech Service Desku ve smyslu a v rozsahu dle článku 6.2 smlouvy;

Výkaz vždy ve vztahu ke **Službám na objednávku** bude obsahovat:

Přehled:

- nevyčerpaná část z limitu Člověkodnů pro poskytování Služeb na objednávku a z maximální celkové Ceny služeb na objednávku;
- seznam účinných Dílčích smluv v měsíci, za který je Výkaz vyhotovován;
- shrnutí provedených činností v rámci jednotlivých Dílčích smluv;
- seznam provedených dílčích částí plnění dle Dílčích smluv;
- uvedení časové náročnosti v Člověkodnech k jednotlivým Dílčím smlouvám;
- shrnutí časové náročnosti v Člověkodnech za všechny Služby na objednávku poskytnuté v daném měsíci a určení výše Ceny služeb na objednávku;
- uvedení členů Realizačního týmu odpovědných za plnění konkrétních Dílčích smluv;

Podrobná část:

- uvedení členů Realizačního týmu, kteří poskytnuli jakékoliv Služby na objednávku s uvedením počtu Člověkohodin (u každého člena) strávených poskytováním Služeb na objednávku a stručného popisu obsahu činnosti takového člena Realizačního týmu za každý Člověkoden (jednalo-li se o kontinuální činnost, pak postačuje uvedení obsahu činnosti a počtu Člověkodnů strávených danou činností).

Výkaz za daný měsíc musí dále vždy obsahovat alespoň**:**

- celkovou délku skutečné kumulované doby nedostupnosti v jednotlivých kalendářních týdnech;
- celkovou délku překročení Reakční doby a Doby vyřešení;
- seznam všech jednotlivých Výpadků a jejich délka;
- výši jednotlivých smluvních pokut k jednotlivým porušením parametrů Služeb dle tohoto dokumentu
- další údaje nezbytné pro řádné a věrné zachycení plnění Paušálních služeb dle požadavku Objednatele

Výkaz bude Objednateli předáván v přehledné tabulce rozdělené na jednotlivé listy, které budou v takové tabulce seřazeny v pořadí:

- Cena paušálních služeb, Cena služeb na objednávku za daný měsíc;
- Přehled poskytnutých Paušálních služeb za daný měsíc;

- Přehled poskytnutých Služeb na objednávku za daný měsíc;
- Podrobná část Paušálních služeb viz požadavek výše;
- Podrobná část Služeb na objednávku viz požadavek výše;

vyjma kompletního záznamu o Úkonech Service Desku, který bude předán **ve formě přehledného logu umožňujícího vyhledávání a uchovávání záznamů o Úkonech Service Desku.**

12. POŽADAVKY NA ŘÍZENÍ PROJEKTU POSKYTOVATELEM

Poskytovatel v rámci dodávky bude zajišťovat projektové řízení. Projektové řízení bude realizované jako konvenční projektové řízení v oblasti ICT v souladu s mezinárodně uznávanou projektovou metodikou (např. Prince 2, IPMA, PMI), Poskytovatel uvede v nabídce i předimplementační analýze využívanou metodiku.

V případě potřeby přechodu Poskytovatele do agilního projektového řízení v určitých fází projektu tak může učinit pouze v odůvodněných případech po informování Objednatele a schválení agilního projektového řízení ze strany Objednatele. V takovém případě bude Poskytovatel postupovat podle uznávané mezinárodní metodiky pro agilní projektové řízení (např. SCRUM, Prince 2 Agile) s informováním Objednatele o užité metodice.

Poskytovatel za projektové řízení, korektní nastavení projektových aktivit nese odpovědnost a bude realizovat aktivity projektového řízení, které se především spočívají v:

- Účastí na pravidelných projektových poradách minimálně o 14denní bázi (Objednatel může v odůvodněných případech schválit pro různé etapy jinou frekvenci jednání)
- Účasti na řídícím výboru projektu
- vedení projektové dokumentace v rozsahu doporučovaném projektovou metodikou,
- realizace zápisů z jednání,
- vedení registru rizik,
- upozornění Objednatele na nová rizika, změnu jejich závažnosti či na informaci, že došlo k aktivaci rizika s uvedením odhadu vlivu na projekt a následným řešením opatření s Objednatelem a jeho partnery,
- koordinace projektu a pracovníků Poskytovatele,
- spolupráci s Objednatelem a jeho partnery dle potřeby,
- zajištění zastupitelnosti klíčových členů projektového týmu Poskytovatele,
- návrh harmonogramu,
- rozpad harmonogramu na etapy,
- dohled harmonogramu,
- bezodkladné informování o ohrožení harmonogramu s dopadem na termíny,
- vedení registru úkolů,
- vedení organizační a komunikační matice,
- rozpad projektových aktivit do WBS a pravidelné informování Objednatele o plnění aktivit dané fáze s uvedením procentuálního plnění aktivity a **s možností předvedení stavu výstupů na vyžádání v rámci nejbližší projektové porady ve všech etapách projektu,**
- vedení procesu změn na úrovni vedoucích pracovníků Objednatele a Poskytovatele,
- vedení procesu předání a akceptace na straně Poskytovatele.

Poskytovatel naplní výše uvedené aktivity a bude pravidelně spolupracovat s Objednatelem a jeho partnery (např. Poskytovatelem infrastruktury Objednatele, poradci, technickým dozorem a technickými správci) na operativní bázi a vyžádání součinnosti.

Veškerou dokumentaci bude Poskytovatel vkládat do sdíleného projektového úložiště, zřízeného Objednatelem (pro neprojektovou dokumentaci ISSV – systémovou, analytickou apod. zvláštní on-

premise úložiště u Objednatele s omezeným přístupem pro vybrané osoby Poskytovatele). Projektová dokumentace bude vedena pro všechny fáze/etapy.

Další povinnosti Poskytovatele spojené s řádným dodání ISSV a souvisejících služeb a výstupů jsou detailně uvedeny v rámci smlouvy a servisní smlouvy.

12.1. HARMONOGRAM REALIZACE

Harmonogram realizace bude v detailu zpracován Poskytovatelem do detailu projektových aktivit a bude reflektovat Objednatelem navržené rozdělení fází a etap, uvedené v subkapitole Požadavky na řízení fází a akceptační kritéria.

Harmonogram musí akceptovat požadované časové alokace pro připomínkování, uvedené v kapitole Požadavky na řízení fází a akceptační kritéria a dále musí akceptovat požadované výstupy a akceptační kritéria fází.

Harmonogram může vhodně přesouvat či slučovat aktivity ve fázích, ale nesmí omezit plnění těchto aktivit ani redukovat jejich výčet či omezit výstupy fází a akceptační kritéria.

Harmonogram musí dodržovat následující termíny předání výstupů fází/fakturační milníky:

- Dokončení fáze Testovací provoz a její akceptace – **31. 12. 2025**
- Dokončení fáze Pilotní provoz a její akceptace – **30. 4. 2026**
- Dokončení fáze Metodické součinnosti a její akceptace – **30. 6. 2026**
- Dokončení fáze doplňování DB partnery a následná akceptace Díla **– 31. 12. 2026**

Do termínů fakturačních milníků musí Poskytovatel řádně předat výstupy fází s jejich řádnou akceptací, což platí pro výstupy všech fází předcházejících danému fakturačnímu milníku.

Za dodržování harmonogramu nese odpovědnost Poskytovatel. V případě, že vinou kterékoli strany, externího aktéra či události může dojít k ohrožení harmonogramu a milníků, je o tomto Poskytovatel povinen Objednatele bezodkladně informovat.

Harmonogram a jeho plnění musí rovněž dodržovat související ustanovení smlouvy.

12.2. ANALÝZA RIZIK PROJEKTU

Poskytovatel zpracuje analýzu rizik projektu a výsledná rizika budou zavedena do registru rizik. Tento registr rizik povede Poskytovatel v rámci sdíleného úložiště s Objednatelem.

Rizika budou ohodnocena pravděpodobností, dopadem, cílovou hodnotou s využitím projektové metodiky nebo metodiky řízení rizik. K ohodnoceným rizikům bude navrženo opatření s odhadem cílové hodnoty rizika po zavedení opatření.

Registr rizik bude pravidelně revidován a v případě změny hodnoty rizika, nalezení nových rizik bude informovat Objednatele. V případě eskalace rizika bude o tomto Poskytovatel informovat neprodleně.

Registr rizik je doporučeno rozdělit dle kategorií rizika, například na rizika:

- Politická
- Organizační
- Lidský faktor
- Technická – ICT, IS, komponenty, DB…
- Finanční
- Konkurence

- Časová – Harmonogram
- Provozní
- Zainteresované strany

Cílový rozšířený výčet kategorií vznikne na základě dohody Objednatele a Poskytovatele.

12.3. SOUČINNOST A KOORDINACE PROJEKTU

V případě vyžádání součinnosti je Poskytovatel povinen reagovat na požadavek dle SLA stanovených ve smlouvě dle kategorie požadavku, např. součinnost při svolání řídícího výboru. Pro požadavky nedefinované smlouvou platí požadovaná reakční doba 4 hodiny v režimu 8x5 s vyřešením běžného požadavku do 48 hodin. V případě zvýšené náročnosti na požadavek je Poskytovatel povinen o tomto informovat Objednatele a navrhnout nejbližší možnou reakční dobu na dotaz či požadavek. Oficiální požadavky smluvních stran (např. na součinnost) budou evidovány v rámci service-desku

Poskytovatel se vyjma pravidelných projektových porad účastní i operativních jednání s Objednatelem do 7 pracovních dnů od výzvy Objednatele, případně je bude sám iniciovat v případě potřeby analytického jednání či vstupních informací.

Komunikace projektových týmů bude probíhat ve věcech projektových a smluvních přes oprávněné osoby. Ve věcech odborných budou moci komunikovat odborní pracovníci mezi sebou s informováním odpovědných osob obou stran. Běžná komunikace bude možná prostřednictvím e-mailu, telefonu, service-desku a dalších komunikačních prostředků. V případě potřeby rozhodnutí bude komunikace vedena e-mailem na úrovni projektových manažerů a evidována v rámci ticket systému service-desku. V případě informace s dopadem na smluvní vztahy bude komunikace vedena přes datové schránky uvedené ve smlouvě a evidována v rámci service-desku. Veškeré změny s dopadem na rozsah, cíl, harmonogram nebo rozpočet musí být projednány řídícím výborem, který má posouzení změn v kompetenci.

Poskytovatel se kromě projektových porad musí účastnit jednání řídícího výboru projektu prostřednictvím osob uvedených ve smlouvě. Řídící výbor bude složen ze zástupců Poskytovatele, Objednatele a jeho partnerů zainteresovaných do projektu. Poskytovatel je na jednáních řídícího výboru povinen poskytovat potřebnou součinnost Objednateli a jeho partnerům, vč. reportingu managementu Objednatele. Z jednání bude Poskytovatel vytvářet zápisy, které budou předmětem schvalování.

Řídící výbor je oprávněn:

- řídit a schvalovat činnost projektového manažera a rozhodovat o změně rozsahu projektu
- potvrzovat zprávy o postupu projektu, status reporty projektového manažera a nastavení projektu;
- činit potřebná rozhodnutí o změně rozsahu Plnění, Harmonogramu, možné změny Ceny (pakliže jsou překročeny limity příslušných změn);
- odpovídá za průběžnou kontrolu realizace projektu a rovněž za dodržování jeho strategického zaměření

Změny rozsahu projektu budou řešeny v souladu s ustanoveními smlouvy.

Vyjma dodržování pravidel běžné komunikace definované v této kapitole musí Poskytovatel do 15 dnů ode dne nabytí účinnosti smlouvy zřídit a po celou dobu realizace a servisní podpory ISSV udržovat v provozu service-desk a udělit náležitá oprávnění k přístupu do service-desku pracovníkům Objednatele a dalším pověřeným uživatelům dle pokynů Objednatele.

Service-desk slouží mimo jiné pro příjem a evidenci požadavků, oznámení o potřebě součinnosti Objednatele a dalších zpráv, potvrzování jejich přijetí, předávání jednotlivých úkolů jednotlivým členům realizačního týmu (případně jiným pověřeným osobám), sledování stavu, průběhu a procesu prací na plnění a dalších zpráv, informování o stavu řešení, vytváření přehledů a statistik o řešených požadavcích a dalších zprávách, a další funkcionality běžné u service-desku. Service-desk bude mít plně logovaný provoz pro zajištění dohledatelnosti přístupů, uživatelských akcí, stavu ticketů v čase apod.

Service-desk bude jak ve fázi realizace projektu, tak při provozu ISSV sloužit k hlášení zjištění, incidentů a při provozu ISSV rovněž pro vkládání požadavků na podporu či rozvoj.

Service-desk bude k dispozici 24x7 a bude obsahovat webové prostředí (s ticketovacím systémem), telefonní linku (hot-line metodického a technického pracovníka) a e-mailové kontaktní adresy.

Objednatel poskytne následující součinnost:

- Účast na školeních
- Zajištění prostor školení
- Zajištění testerů
- Konzultace v metodické i technické oblasti v nezbytném rozsahu pro řádné vytvoření a dodání ISSV a souvisejících služeb v rozsahu 2FTE
- Zajištění infrastruktury pro ISSV, vytvoření testovacího a produkčního prostředí pro instance ISSV
- Zajištění součinnosti třetích stran v oblasti integrací a sdílení dat
- Zajištění vstupních informací o integračních rozhraních třetích stran
- Informování Poskytovatele o konfiguraci ICT prostředí ISSV
- Informování Poskytovatele o odstávkách ICT prostředí

12.4. POŽADAVKY NA ŘÍZENÍ FÁZÍ A AKCEPTAČNÍ KRITÉRIA

Níže je uveden doporučený popis fází, jejich řízení a akceptační kritéria. Fázování může Poskytovatel v rámci návrhu harmonogramu pozměnit, akceptační kritéria jsou neměnná.

Akceptace výstupů projektu se procesně řídí pravidly akceptace, stanovenými ve smlouvě a v případě fáze provozu se akceptace rozvojových i paušálních služeb řídí procesem a podmínkami akceptace, stanovenými v servisní smlouvě.

ETAPA 1

12.4.1. FÁZE ZPRACOVÁNÍ CÍLOVÉHO KONCEPTU

Cílem fáze je započetí projektové spolupráce a vytvoření předimplementační analýzy. V této fázi po podpisu smlouvy bude realizováno společné jednání Objednatele a Poskytovatele s cílem nastavení projektové spolupráce a následně bude Poskytovatel na dalším jednání představen partnerům Objednatele. Na základě těchto jednání bude vytvořena organizační a komunikační matice a rovněž bude vytvořena či aktualizovaná projektová dokumentace z nabídky – harmonogram, registr rizik, WBS a další uvedená výše.

Následně budou v rámci zpracování analýzy Poskytovateli Objednatelem poskytnuty dostupné dokumenty k ISSV a bude mu poskytnuta součinnost s případnými dotazy k detailu ISSV jak od Objednatele, tak jeho partnerů.

Vytvářená předimplementační analýza musí obsahovat požadavky uvedené v tomto dokumentu a bude pravidelně komunikovaná s Objednatelem na projektových poradách. V případě potřeby technické diskuse zajistí Objednatel účast rovněž partnerů Objednatele.

Po vytvoření předimplemenční analýzy bude dokument prezentován Objednateli a bude předán k připomínkování. Dokument bude připomínkován Objednatelem a jeho partnery minimálně 21 kalendářních dní. Následně budou připomínky předány Poskytovateli k jejich vypořádání. Ten provede jejich vypořádání do 14 kalendářních dní. Poskytovateli je doporučeno diskutovat stav předimplementační analýzy průběžně před předáním, aby nedošlo k prodlevám v rámci připomínkovacího řízení.

Po vypořádání připomínek proběhne akceptační řízení předimplementační analýzy. Předimplementační analýza je závazná pro následnou fázi realizace a bude dále upřesněna v rámci realizace, přičemž výstupy a závěry analýzy budou implementovány do systémové dokumentace ISSV.

Akceptační kritérium: Předaná předimplementační analýza v souladu s požadavky této technické specifikace.

12.4.2. FÁZE REALIZACE

V této fázi dojde k vytvoření samotného ISSV. Poskytovatel vytvoří na vlastní náklad vývojové prostředí, které bude minimálně po dobu závěrečných testů etapy parametrově simulovat jedno z cílových prostředí – testovací či produkční. V rámci prostředí Poskytovatele bude vytvářen ISSV. Poskytovatel bude vytvářet systém se zajištěním důvěrnosti a bezpečnosti ISSV již v rámci vývojového prostředí. V rámci vývoje budou rovněž připracovány integrace, jejich cílová konfigurace bude realizovaná v následující fázi. ISSV bude naplněn testovacími daty pro otestování DB a vhodnosti datové struktury. Objednatel zajistí součinnost Poskytovatelů /správců integrovaných SW.

I během této fáze budou realizované pravidelné projektové porady s Objednatelem s cílem informování o postupu na vyvíjeném ISSV. Objednatel má právo kdykoli požádat o asistovaný přístup do vývojového prostředí a náhled na současnou podobu ISSV.

Poskytovatel již ve vývojovém prostředí bude realizovat úvodní sérii testů – performance, penetrační testy a aplikační testy vlastním týmem. O výsledcích testů bude informovat Objednatele a doloží protokoly z testování.

Na závěr realizace bude Poskytovatel prezentovat ISSV v prostředí Poskytovatele a předloží aktualizovanou verzi předimplemenční analýzy, především s ohledem na systémové požadavky a průběh implementace.

K výstupům fáze proběhne akceptační řízení s Poskytovatelem s minimální časovou alokací 14 kalendářních dní na připomínky a 7 kalendářních dní na vypořádání připomínek.

Akceptační kritérium: Předaná aktualizovaná předimplementační analýza v souladu s požadavky této technické specifikace, protokoly z testování, funkční ISSV v prostředí Poskytovatele s nasazenou integrační platformou.

12.4.3. FÁZE IMPLEMENTACE

Cílem fáze je implementace ISSV do testovacího prostředí na infrastruktuře Poskytovatele infrastruktury Objednatele. Během této fáze budou realizované pravidelné projektové porady s Objednatelem s cílem jeho informování a dále porady s Poskytovatelem infrastruktury Objednatele pro koordinaci nasazení ISSV do testovacího prostředí na infrastruktuře Poskytovatele infrastruktury.

Před samotným nasazením bude Poskytovatelem infrastruktury Objednatele připravena infrastruktura a technologický SW, vč. nastavených operačních systému a databází v souladu s požadavky předimplementační analýzy. Ta musí reflektovat katalog služeb Poskytovatele infrastruktury, alternativně schválené výjimky Objednatelem a Poskytovatelem infrastruktury. V případě potřeby

součinnosti ze strany Poskytovatele poskytne Poskytovatel součinnost v potřebném rozsahu pro správné škálování a konfiguraci infrastruktury a testovacího prostředí.

Do tohoto prostředí bude implementován ISSV za součinnosti Poskytovatele a Poskytovatele infrastruktury Objednatele či dalších technických správců. Poskytovatel je odpovědný za nasazení ISSV a jeho funkčnost, Poskytovatel infrastruktury za konfiguraci kybernutes, potažmo virtualizace, operačního systému a databázového serveru, nastavení kapacitního HW výkonu, diskové kapacity a související služby monitoringu infrastruktury a bezpečnosti.

Po nasazení bude systém naplněn cílovými daty, minimálně testovacími daty ZR (data modulu seznam voličů budou finalizována až ve fázi Doplňování DB partnery) a bude realizované napojení na integrované SW a registry, definované v této technické specifikaci, případně rozšířené o výsledky předimplementační analýzy. Dojde k iniciálnímu otestování funkčnosti Poskytovatele a bude umožněn přístup vybraných pracovníků Objednatele do ISSV.

O nasazení ISSV do testovacího prostředí bude k dispozici zpráva, která bude potvrzovat funkčnost a bezpečnost ISSV, naplněnou databází v cílové struktuře a rozsahu v souladu s předimplementační analýzou a touto technickou specifikací a výsledcích provedených inicializačních testů – aplikační testy vč. otestování integrací.

Vyjma výše uvedeného Poskytovatel vytvoření testovací scénáře pro jednotlivé testy. Ty budou dodány společně s ostatním Objednateli k akceptaci.

K výstupům fáze proběhne akceptační řízení s minimální časovou alokací 14 kalendářních dní na připomínky a 7 kalendářních dní na vypořádání připomínek Předmětem akceptace bude zpráva nasazení ISSV, testovací scénáře a nezávislé ověření Objednatelem, že je ISSV korektně nasazen v prostředí Poskytovatele infrastruktury Objednatele.

Akceptační kritérium: Zpráva o nasazení ISSV v testovacím prostředí, ověření nasazení Objednatelem, testovací scénáře.

12.4.4. FÁZE TESTOVACÍ PROVOZ

Cílem fáze je otestování hotového a konfigurovaného ISSV. Během této fáze budou realizované pravidelné projektové porady s Objednatelem s cílem jeho informování a dále testovací schůzky s testery Objednatele.

Před otestováním ISSV zajistí Poskytovatel školení testerů Objednatele do takové míry, aby bylo možné testy simulovat uživatele při realizaci procesů v ISSV dle jednotlivých rolí. Ze školení vznikne rovněž videozáznam, který bude předán Objednateli.

V rámci fáze dojde k důkladnému testování ISSV v testovacím prostředí. Bude realizovaná kompletní série testů, uvedená v této technické specifikaci. Na základě výsledků testů budou vystaveny testovací protokoly.

Pokud budou v testovacích protokolech nalezeny neshody oproti požadovanému stavu, bude situace řešena formou oprav ISSV Poskytovatelem a jejich nasazení do testovacího prostředí k opětovnému otestování.

V této fázi proběhnou minimálně dvě kola kompletního otestování ISSV. V případě potřeby realizace dalších kol testování v důsledku chyb ISSV, potažmo Poskytovatele, budou tyto kola prodloužením fáze vinou Poskytovatele, který musí uzpůsobit další fáze této prodlevě, například navýšením HR kapacit. Rovněž mohou být tyto prodlevy předmětem sankcí Objednatele v souladu se smlouvou.

Po vystavení protokolů ze všech testů s výsledkem bez chyby bude Poskytovatelem vytvořena zpráva z testování, která bude předána Objednateli. Pokud došlo k úpravám ISSV v důsledku oprav po otestování, budou tyto změny propsány do předimplementační analýzy.

Poskytovateli je doporučeno alokovat pro fázi minimálně 2 měsíce pro komplexní řádné otestování IS v souladu s požadavky tohoto dokumentu.

K výstupům fáze proběhne akceptační řízení s minimální časovou alokací 7 kalendářních dní na připomínky a 7 kalendářních dní na vypořádání připomínek Předmětem akceptace bude zpráva o nasazení ISSV, testovací scénáře a nezávislé ověření Objednatelem, že je ISSV korektně nasazen v prostředí Poskytovatele infrastruktury Objednatele.

Akceptační kritérium: Realizované školení testerů (záznam), Výsledná zpráva z testování, aktualizovaná verze předimplementační analýzy.

Termín dokončení: 31. 12. 2025

12.4.4.1. Fakturační milník 1

Po dokončení fáze testovací provoz a splnění akceptačních kritérií této fáze bude Poskytovatel fakturovat poskytnuté služby a dodávky.

ETAPA 2

12.4.5. FÁZE IMPLEMENTACE DO PRODUKCE

Cílem fáze je nasazení otestovaného ISSV do produkce. Během této fáze budou realizované pravidelné projektové porady s Objednatelem s cílem jeho informování a dále porady s Poskytovatelem infrastruktury Objednatele pro koordinaci nasazení ISSV do preprodukčního a produkčního prostředí na infrastruktuře Poskytovatele infrastruktury.

Vhodným technologickým způsobem, jenž stanoví Poskytovatel za součinnosti Poskytovatele infrastruktury Objednatele a Objednatele bude implementovaný ISSV do preprodukčního a produkčního prostředí. Pokud bude třeba realizovat změny konfigurací, integračních prostupů, či jiné modifikace ISSV, budou tyto změny realizované Poskytovatelem.

Následně po nasazení bude systém rámcově otestován jak Poskytovatelem, tak Objednatelem s využitím existujících testovacích scénářů z minulé fáze. Pokud budou testy úspěšné, bude ISSV považován za systém v produkčním provozu, který bude začínat asistovaným pilotním provozem. O nasazení ISSV do produkčního prostředí a úspěšném otestování bude k dispozici zpráva, která bude potvrzovat funkčnost a bezpečnost ISSV v preprodukčním a produkčním prostředí a bude předána Objednateli.

Poskytovatel v rámci fáze provede cílová školení, jak správců, tak uživatelů. Rovněž vytvoří finální školící materiály a předá je Objednateli.

V této fázi Poskytovatel vytvoří a předá Objednateli finální systémovou dokumentaci v rozsahu požadovaném pro ISVS dle zákona 365/2000 Sb., součástí předání budou kompletní zdrojové kódy v souladu s požadavky této technické specifikace.

K výstupům fáze proběhne akceptační řízení s minimální časovou alokací 14 kalendářních dní na připomínky a 7 kalendářních dní na vypořádání připomínek Předmětem akceptace bude zpráva o nasazení ISSV, systémová dokumentace a zdrojové kódy, realizovaná školení a školící dokumentace.

Akceptační kritérium: Realizované školení správců a uživatelů, školící dokumentace, systémová dokumentace, zdrojové kódy, zpráva o nasazení ISSV v preprodukčním a produkčním prostředí

12.4.6. FÁZE PILOTNÍ PROVOZ

Cílem pilotního provozu je praktické otestování ISSV v provozu. Během pilotního provozu bude systém již veřejně dostupný a rutinně fungující. Tato fáze je součástí realizace projektu a je zavedena s cílem garance bezproblémového chodu a nalezení možných chyb, které neodhalily předchozí fáze.

Předpokladem je, že realizace pilotního provozu bude spojena s konáním tzv. nových a dodatečných voleb do zastupitelstev obcí, které se budou konat na začátku dubna 2026. Tento typ voleb se bude konat ve velmi omezeném počtu obcí a umožní tak na tomto malém vzorku realizovat pilotní realizaci všech nezbytných úkonů v rámci IS již v ostrém provozu.

Během pilotního provozu budou realizované jednání na minimálně na týdenní bázi a v případě potřeby s účastí Poskytovatele do 1 pracovního dne od vyzvání. Během této doby bude Poskytovatelem poskytována nepřetržitá podpora se zvýšenou mírou podpory a řešením požadavků Objednatele se shodnými SLA jako v případě provozu v režimu Příprava voleb nebo Volby.

Pilotní provoz je stanoven na minimálně 75 kalendářních dnů.

Po uplynutí doby a vyřešení nalezených zjištění proběhne akceptační řízení s minimální časovou alokací 7 kalendářních dní na připomínky a 7 kalendářních dní na vypořádání připomínek Předmětem akceptace bude zpráva o pilotním provozu ISSV, seznam případných změn a vyřešených incidentů, aktualizovaná dokumentace a zdrojové kódy.

Akceptační kritérium: Akceptace pilotního provozu (ISSV v produkčním provozu po pilotním provozu), vč. seznamu případných změn a vyřešených incidentů, aktualizovaná dokumentace a zdrojové kódy

Termín dokončení: 30. 4. 2026

12.4.6.1. Fakturační milník 2

Po dokončení fáze pilotní provoz a splnění akceptačních kritérií této fáze bude Poskytovatel fakturovat poskytnuté služby a dodávky.

12.4.7. FÁZE METODICKÉ SOUČINNOSTI

Ve fázi dojde k zajištění metodické podpory dotčeným subjektům ISSV, které bude pro úspěšné využití ISSV v praxi.

Z hlediska státní správy budou uživateli IS vedle Ministerstva vnitra v různé míře všechny obecní úřady, krajské úřady, Ministerstvo zahraničních věcí (včetně zastupitelských úřadů) a Český statistický úřad.

Úspěšně zrealizovaná metodická podpora bude garantovat bezproblémovou využitelnost a funkčnost IS k jednotlivým úkonům, které budou jeho prostřednictvím zajišťovány, a které jsou nezbytné pro řádnou realizaci volebního procesu v České republice.

Poskytovatel v této fázi stejně jako v předchozích bude řešit případné incidenty a omezení funkčnosti ISSV a dále bude poskytovat metodickou součinnost nejen Objednateli, ale rovněž se účastní metodických workshopů a školení Objednatele, realizovaného pro obce a další zainteresované strany projektu, kde bude prezentovat funkcionality ISSV, poskytne nezbytnou podporu zapojeným subjektům, případně doplní uživatelskou dokumentaci o zjednodušené metodické postupy pro procesy v ISSV.

Cílem je kromě zajištění možnosti spolupráce s dalšími subjekty v ISSV zaškolení uživatelů obcí ve vkládání dat do ISSV s ohledem na další fázi – pro tuto potřebu bude využita již existující školící dokumentace a záznamy školení, nicméně v případě potřeby Objednatel může realizovat samostatné školení na vkládání dat, na kterém by Poskytovatel participoval jako další lektor.

K výstupům fáze proběhne akceptační řízení s minimální časovou alokací 7 kalendářních dní na připomínky a 7 kalendářních dní na vypořádání připomínek Předmětem akceptace bude výkaz o poskytnuté součinnosti a doplňující uživatelská dokumentace.

Akceptační kritérium: Akceptace poskytnuté metodické součinnosti, aktualizovaná uživatelská dokumentace

Termín dokončení: 30. 6. 2026

12.4.7.1. Fakturační milník 3

Po dokončení fáze metodické součinnosti a splnění akceptačních kritérií této fáze bude Poskytovatel fakturovat poskytnuté služby a dodávky.

12.4.8. FÁZE DOPLŇOVÁNÍ DB PARTNERY

V této fázi proběhne rozšiřování datového fondu ISSV o vstupní informace od obcí a dále k metodickému vedení obcí při využívání ISSV a rozvoji datového fondu. V průběhu fáze dojde k rozšíření databáze, konkrétně dat ROB a RUIAN. DB seznamu voličů bude rozšířena o další data od obcí (atributy nad rámec ROB). Pro tyto data bude již existovat struktura DB, tedy dojde pouze k doplňování dat do existujících tabulek.

Poskytovatel v této fázi stejně jako v předchozích bude řešit případné incidenty a omezení funkčnosti ISSV a dále bude poskytovat metodickou součinnost nejen Objednateli, ale rovněž zapojeným subjektům, které budou přistupovat do ISSV. Součinnost bude v této fázi zaměřena na pomoc uživatelům vkládat data do registru voličů a případné komplikace.

Jelikož bude v této fázi vstupovat do ISSV více uživatelů různých subjektů (primárně obce) v roli editora, existuje zvýšené riziko, že může dojít k neočekávaným stavům na straně editorů ISSV a bude proto velký důraz kladen na řešení incidentů a zajištění funkčnosti, dostupnosti a konzistence DB.

12.4.8.1. AKCEPTACE DÍLA

Po akceptaci ze strany Objednatele je realizační část projektu považována za úspěšně ukončenou a může započít poskytování servisních služeb Poskytovatele.

K výstupům fáze proběhne akceptační řízení s minimální časovou alokací 7 kalendářních dní na připomínky a 7 kalendářních dní na vypořádání připomínek. Akceptuje se Dílo vč. aktualizovaných výstupů níže.

Akceptační kritérium: Akceptace poskytnuté součinnosti při doplňování DB ISSV, akceptace ISSV (akceptační protokol realizační fáze + přílohy v případě jejich změn – finální systémová dokumentace, zdrojové kódy, poslední testovací protokoly, školící dokumentace)

Termín dokončení: 31. 12. 2026

12.4.8.2. Fakturační milník 4

Po dokončení fáze akceptace Díla a splnění akceptačních kritérií této fáze bude Poskytovatel fakturovat poskytnuté služby a dodávky.

12.4.9. PROVOZNÍ FÁZE

Provozní fáze následuje po samotné realizaci projektu dodání ISSV. Během této fáze, která je nastavena na 5 let od akceptace Díla budou Poskytovatelem poskytovány služby servisní podpory a rozvoje ISSV na základě objednávek Objednatele v souladu se smlouvami a přílohami smluv.

Akceptační kritérium: Výkazy poskytovaných služeb (servisní služby), akceptační protokoly k objednávkám (rozvojové práce)

13. PŘÍLOHY

Příloha č. 1 - Popis požadavků na analýzu a realizaci napojení na DCeGOV

PŘÍLOHA Č. 1- POPIS POŽADAVKŮ NA ANALÝZU A REALIZACI NAPOJENÍ NA DCeGOV

Tento dokument popisuje požadavky na součinnost Poskytovatele při vypracování analýzy napojení ISSV na DCeGOV v rámci předimplementační analýzy ISSV a případnou následnou realizaci faktického napojení ISSV na DCeGOV.

POPIS SLUŽEB DCeGOV

Dohledové centrum eGovernmentu poskytuje soubor služeb, které lze kategorizovat dle ustanovení VyKB:

- V souladu s požadavky § 14 Zvládání kybernetických bezpečnostních událostí a incidentů:
    - detekce kybernetických bezpečnostních událostí,
    - posuzování kybernetických bezpečnostních událostí, při kterém musí být rozhodnuto, zda mají být klasifikovány jako kybernetické bezpečnostní incidenty,
    - prošetření a určení příčin kybernetického bezpečnostního incidentu.
- V souladu s § 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů:
    - sběr specifických kategorií provozních a bezpečnostních událostí z vybraných technických aktiv připojených systémů.
- V souladu s požadavky § 23 Detekce kybernetických bezpečnostních událostí:
    - detekce kybernetických bezpečnostních událostí nad souborem zpracovávaných provozních a bezpečnostních událostí.
- V souladu s požadavky § 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí:
    - vyhodnocování kybernetických bezpečnostních událostí,
    - identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.

POŽADAVKY NA POSKYTOVÁNÍ UDÁLOSTÍ DO DCeGOV

Systém loguje své činnosti a činnosti uživatelů (aplikační logování), včetně administrátorů do strukturovaných logů.

Všechny užité komponenty aplikační architektury ISSV (ty jsou zároveň technickými podpůrnými aktivy) musí umožňovat předávání logovací zprávy (tomu musí odpovídat licence případného Standardního SW užitého v aplikační architektuře ISSV), pokud to Poskytovatelem použité prvky nativně nepodporují, je v odpovědnosti Poskytovatele tuto funkcionalitu odpovídajícím způsobem zajistit; na míru naprogramované komponenty musí být realizovány tak, že budou umožňovat předávání logovací zprávy na SIEM DCeGOV.

Systém loguje uživatelskou aktivitu pro všechny role. V rámci těchto logů jsou zaznamenávány takové atributy, aby šlo jednoznačně identifikovat:

- čas provedení,

- provádějící identitu/účet,
- provedenou akci
- dotčená data (entitu, záznam).

Logy jsou ukládány po dobu alespoň 18 měsíců.

Nastavení doporučené úrovně auditního logování je uvedeno v ISMS 03.01.11.P01.P01 Doporučené nastavení logování technologických komponent.

Způsob transportu událostí je definován formou POST – zasíláním událostí na sběrné místo – kolektor nebo GET – události jsou vyčítány z podpůrného technického aktiva.

V případě existujícího konektoru a podporovaného nebo certifikovaného konektoru výrobcem technického prostředku bezpečnosti provozovaného DCeGOV (SIEM ArcSight) je využit SmartConnector, **tento způsob je Objednatelem preferován**. Objednatel připouští také jiné způsoby propojení, kdy je nutné provést na straně DCeGOV vývoj konektoru zajišťující normalizaci a parsování - tzv. FlexConnector, což generuje náklady na straně Objednatele.

Samotný vývoj je prováděn na základě poskytnutých vzorových událostí z napojovaného informačního systému, který bude obsahovat všechny typy událostí dle VyKB §22 odst. 2., písm. d), a také detailní dokumentaci týkající se logování (Seznam vzorových událostí a jejich dalšího popisu zpracuje Poskytovatel).

Pro zdroje událostí, které využívají syslog protokol, musejí být tyto předány v nepozměněném tvaru (tzv. RAW formátu) na Loadbalancer v lokalitě NDC kterou určí Objednatel. Pro každou technologii je nutné použít separátní syslog TCP kanál. Dle standardu DCeGOV začíná příjem od portu 8600/TCP a výše.

DNS resolving – DNS dotazy v architektuře SIEM ArcSight – preferovaný způsob – zdroj logů (ISSV) uvede do zalogované zprávy svou hostname i IP adresu.

Na DCeGOV musí být napojena všechna prostředí ISSV (vývojové, testovací, preprodukční, produkční).

VÝSTUPY ZPRACOVANÉ POSKYTOVATELEM ZA ÚČELEM NAPOJENÍ ISSV NA DCeGOV

- Realizace analýzy integrace na DCeGOV v detailu požadovaném dle dokumentu technické specifikace ISSV, jehož přílohou je tento dokument součástí
- Zakomponování analýzy integrace na DCeGOV do předimplementační analýzy ISSV a provázání ve zkoumaných oblastech analýzy – tedy např. do architektury, popisů modularity a integrací, popisu procesů, bezpečnostní části předimplementační analýzy, dále v rámci analýzy aktiv a rizik.
- Realizace integrační vazby v případě rozhodnutí Objednatele o realizaci na bázi služeb na objednávku v průběhu vytváření Díla. Realizace bude dodržovat stejný harmonogram jako zbytek integrací, viz. kap. Požadavky na řízení fází a akceptační kritéria dokumentu technické specifikace ISSV.

POŽADOVANÁ SOUČINNOST PŘI NAPOJOVÁNÍ ISSV NA DCeGOV

Realizace analýzy napojení ISSV na DCeGOV:

1. Poskytovatel bude realizovat analýzu v rámci dodání Díla a rozpočtu na dodání Díla

2. Účast na jednáních týmu bude probíhat dle požadavků technické specifikace ISSV za účasti referenčních pracovníků Poskytovatele uvedených ve smlouvě.

3. Připomínkování a zapracování připomínek bude řešeno v rámci předimplementační analýzy ISSV

Realizace vlastního napojení ISSV na DCeGOV:

1. Poskytovatel bude realizovat napojení Díla na DCeGOV v případě rozhodnutí Objednatele a vystavení objednávky v souladu se smlouvou.

2. Poskytovatel bude následně po akceptaci nabídky Objednatelem realizovat napojení na DCeGov a realizaci logování všech podpůrných aktiv a související ladění – technicko-organizační provedení všech potřebných aktivit na straně ISSV a navazující uvedení do provozu, kdy cílem je funkční komunikace mezi ISSV a DCeGOV a funkční logování provedené dle schválené předimpelementační analýzy ISSV a v souladu s požadavky technické specifikace ISSV. Součástí je součinnost s Objednatelem, Poskytovatelem Infrastruktury Objednatele a technickým týmem DCeGOV.

3. Účast na jednáních týmu, který bude provádět aktivity nezbytné pro funkční propojení mezi ISSV a DCeGOV za účasti pracovníků Poskytovatele uvedených ve smlouvě.

4. Připojení k DCeGOV a související konfigurace, součinnost při definici prostupů do DCeGOV.

5. Ověření a nastavení všech auditování technických podpůrných aktiv specifikovaných v předimplementační analýze a analýze aktiv a rizik.

6. Dodání detailního vzorku událostí a dokumentace výrobce specifikujících datové věty pro technická podpůrná aktiva vyžadující vývoj FlexConnectoru s událostmi dle VyKB §22 odst. 2., písm. d) a to se stavy minimálně úspěch/neúspěch/chyba.