SMLOUVA O POSKYTOVÁNÍ SERVISNÍ PODPORY A PROVOZNÍ ÚDRŽBY APLIKACÍ KESSL a EPVDS V LETECH 2024 – 2027

uzavřená podle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
(dále jen „občanský zákoník“)

Číslo smlouvy Objednatele: ČÚZK-52641/2023

Číslo smlouvy Dodavatele:

Smluvní strany

Objednatel:	**ČR - Český úřad zeměměřický a katastrální**
Se sídlem:	Pod sídlištěm 1800/9, 182 11 Praha 8
Jejíž jménem jedná:	Ing. Karel Štencel, místopředseda
IČO:	00025712
ID DS:	uuaaatg

(dále jen „Objednatel“)

a

Dodavatel:	Aplis Solutions s.r.o.
Se sídlem:	Revoluční 767/25, 110 00 Praha 1
Zastoupená:	Petar Petkov Stanchev
Zapsaná:	v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka C 202208
IČO:	29127548
DIČ:	CZ29127548
ID DS:	icbpyhx

(dále jen „Dodavatel“)

uzavírají níže uvedeného dne smlouvu za níže uvedených podmínek.

1 Předmět plnění

1. Předmětem této smlouvy (dále jen „Smlouva“) je zajištění:

   a) Servisní podpory a provozní údržby KESSL (Komplexní elektronická spisová služba) pro Český úřad zeměměřický a katastrální, Zeměměřický úřad, 14 katastrálních úřadů a 7 zeměměřických a katastrálních inspektorátů a jejího podsystému EPVDS (Elektronická podatelna a výpravna v návaznosti na systém datových schránek) pro 94 katastrálních pracovišť. KESSL v resortu Objednatele zajišťuje elektronickou spisovou službu včetně funkcí podatelny a výpravny pro všechna podání na všech resortních orgánech. KESSL je napojen na okolní agendové systémy – interní – ISKN (Informační systém katastru nemovitostí), DMS (Dokument management systém), EIS (Ekonomický informační systém), DMVS (Digitální mapa veřejné správy), systém elektronické pošty (email podatelen), externí – ISDS (Informační systém datových schránek), IK MPSV (Identifikátor Ministerstva práce a sociálních věcí) a RS (Registr smluv).
   b) Služeb na objednávku zejména dle potřeb napojených informačních systému, uživatelů a legislativních změn.

   (dále jen „Plnění“), to vše v rozsahu a za podmínek uvedených v této Smlouvě, jejích přílohách, zadávací dokumentaci k veřejné zakázce „Poskytování servisní podpory a provozní údržby aplikací KESSL a EPVDS v letech 2024 – 2027“ a nabídce Dodavatele předložené v rámci této veřejné zakázky. Plnění bude Dodavatel provádět na profesionální úrovni v kvalitě odpovídající všeobecně uznávaným standardům pro daný okruh činností.

2. Dodavatel se zavazuje poskytovat Objednateli Plnění dle této Smlouvy a jejich případných platných dodatků. Dodavatel poskytne jako součást svého Plnění Objednateli i veškeré doklady potřebné k užívání Plnění (návody, technické dokumenty, záruční listy atp.).

3. Objednatel se tímto zavazuje za podmínek stanovených touto Smlouvou Plnění včetně průvodních dokladů převzít a zaplatit za ně Dodavateli cenu stanovenou v této Smlouvě.

4. Obsahem tohoto závazkového vztahu jsou všechny podmínky, práva a povinnosti stanovené v zadávací dokumentaci a jejich přílohách a nabídce Dodavatele i v případě, že nejsou touto Smlouvou výslovně uvedeny.

5. Smluvní strany prohlašují, že tuto Smlouvu, jakož i jednotlivá práva a povinnosti z ní vyplývající, budou vykládat v souladu se zadávacími podmínkami veřejné zakázky a nabídkou Dodavatele předloženou v rámci tohoto zadávacího řízení.

6. Dodavatel odpovídá za to, že poskytnuté Plnění bude ke dni předání splňovat funkční specifikaci stanovenou zadávací dokumentací, jeho nabídkou do zadávacího řízení a Smlouvou, bude implementováno a provozuschopné v prostředí Objednatele a bude mít příslušnou dokumentaci.

7. Dodavatel se zavazuje zajistit, že pro poskytování Plnění dle Smlouvy 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.

8. Pro realizaci Plnění má Dodavatel právo použít smluvní poddodavatele. Seznam poddodavatelů předložil Dodavatel před podpisem této Smlouvy. Dodavatel má právo použít k Plnění i další poddodavatele po předchozím odsouhlasení Objednatelem. Objednatel odsouhlasení nového poddodavatele bezdůvodně neodmítne. V případě, že Dodavatel využívá poddodavatele k výkonu činností vymezených v této Smlouvě, odpovídá za kvalitu, bezpečnost a včasnost plnění stejným způsobem, jako by činnost prováděl sám.

9. V případě, že Dodavatel využívá poddodavatele k výkonu činností definovaných touto Smlouvou, je povinen informovat poddodavatele o požadavcích na bezpečnost informací a bezpečnostních pravidlech, které je povinen dodržovat při výkonu dané činnosti alespoň ve stejném rozsahu, v jakém to Objednatel požaduje od Dodavatele.

10. Dodavatel bere na vědomí, že Plnění může být a bude používáno i další organizační složkou státu (OSS) z resortu Objednatele.

11. Uplatní-li třetí osoba vůči Objednateli před soudem nebo mimo soud jakékoli své nároky k Plnění či jeho části (zejména v oblasti práv duševního vlastnictví, jako například patentových a autorských práv a obchodních značek) Dodavatel bude Objednatele před těmito nároky bránit a důvodné nároky třetí osoby na vlastní náklady bez zbytečného odkladu vypořádá, případně zajistí na vlastní náklady právní servis/zastupování v obvyklé výši pro Objednatele k jeho obraně. Vypořádání, právní servis/zastupování bude poskytnuto v případě, že Dodavatel bude neprodleně písemně informován Objednatelem o nároku uplatněném třetí stranou a budou mu ze strany Objednatele poskytnuty potřebné informace a součinnost. Dodavatel se také zavazuje v této souvislosti uhradit případné veškeré škody, pokuty, náklady apod., které bude Objednatel povinen v důsledku výše uvedeného uhradit.

12. Objednatel v souladu s ustanovením § 6 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, trvá na dodržování zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací ve smyslu daného zákona. S ohledem na charakter zakázky Objednatel zejména požaduje po Dodavateli, aby v průběhu Plnění této Smlouvy dodržoval a zajistil dodržování pracovněprávních předpisů (zejména zákoníku práce a zákona o zaměstnanosti) vůči všem osobám, které se na Plnění této Smlouvy budou podílet. Dodavatel se zavazuje, že bude dodržovat veškeré povinnosti vyplývající z právních předpisů České republiky, zejména pak z předpisů pracovněprávních, předpisů z oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod., a to vůči všem osobám, které se na plnění veřejné zakázky podílejí, a to včetně poddodavatelů; a v případě požadavku Objednatele mu dodržování daných povinností doloží. Dodavatel je také povinen využít u použitých obalů recyklovatelný materiál, nebo materiál z obnovitelných zdrojů, nebo obalový systém pro opakované použití a zajistit ekologickou likvidaci případného elektro a ostatního odpadu.

2 Rozsah služeb Servisní podpory a provozní údržby

1. Paušální služby Servisní podpory a provozní údržby jsou služby Dodavatele, ve které se Dodavatel zavazuje za podmínek a cen v této smlouvě uvedených:

   a) Poskytovat update a upgrade KESSL vzniklé samostatnou, inovační činností Dodavatele, a to včetně změn vyvolaných legislativními požadavky vyplývajících ze souvisejících nařízení EU, zákonů, vyhlášek a metodik.
   b) Identifikovat a kategorizovat požadavky a vady, a následné opravy KESSL zařazovat do příslušné verze patche KESSL. Identifikací požadavku se rozumí analýza příčin problému nahlášeného Objednatelem, včetně návrhu základního způsobu řešení bez ohledu na to, zda se jedná o vadu systému KESSL, HW, souvisejícího SW nebo jinou vadu. Kategorizací se rozumí i stanovení, zda jde o vadu KESSL, a to buď v části, která nebyla modifikována v rámci plnění dle této Smlouvy, nebo v části již modifikované v rámci plnění dle této Smlouvy.
   c) Zajišťovat záruční servis, tedy odstraňovat Objednatelem řádně nahlášené záruční vady a kritické vady postupem dle čl. 11 Smlouvy.
   d) Poskytovat služby průběžné údržby do celkového rozsahu 7 ČLD měsíčně (nevyužité ČLD z daného měsíce se převádějí do dalšího kalendářního měsíce. Tento převod je převáděn vždy pouze v daném fakturačním období). Všechny vykazované činnosti musí být zaznamenány v Helpdeskovém systému (HD) Objednatele i Dodavatele. Dodavatel je povinen předložit měsíční výkaz práce, který je přílohou této Smlouvy, k odsouhlasení vždy do 15. v následujícím měsíci Zástupci Objednatele. Mezi služby průběžné údržby patří:
      i. odstranit Objednatelem řádně nahlášené nezáruční vady a řešit požadavky, které souvisejí s provozem aplikace KESSL, a které byly způsobeny nesprávnou funkcí KESSL či její části;
      ii. poskytovat součinnost při ověření nových verzí KESSL na referenčním pracovišti (RP) Objednatele;
      iii. poskytovat součinnost při instalaci nových verzí KESSL na produkční prostředí, přičemž termín instalace bude stanoven na základě společné dohody mezi Objednatelem a Dodavatelem;
      iv. poskytovat Technickou podporu (Hot Line) - službu umožňující určeným zástupcům Objednatele konzultovat požadavky související s podporovaným systémem aplikací KESSL;
      v. poskytovat součinnost při realizaci projektů DMS, ISKN, EIS a exchangový klient resortních podatelen, na něž je KESSL integrován.
   e) Vést projekt a účastnit se projektových schůzek – pravidelná jednání 1x za dva týdny výkonný výbor KESSL, 1x za šest týdnů řídící výbor KESSL, a to v budově Objednatele, popřípadě pomocí vzdálené schůzky online. Bližší pravidla řízení projektu (jednotlivé řídící struktury včetně obsazení ŘV a VV, odpovědnost, postupy odsouhlasení zápisů atd.) si smluvní strany dohodnou nejpozději do 1 měsíce po účinnosti Smlouvy. Účast na projektovém vedení (ŘV, VV) se nevykazuje do výkazu za průběžnou údržbu KESSL.

f) Monitorovat provoz. Dodavatel se zavazuje (při dodávkách nových verzí KESSL, případně i při instalacích opravných a změnových patchů) předat monitorovací nástroje (skripty) pro monitorování provozu, a to zejména v období před instalací nové verze, instalace opravného nebo změnového patche KESSL do provozního prostředí, či v období po zavádění zcela nové funkčnosti, s tím, že monitorovány budou zejména oblasti/aplikace KESSL, které jsou v rámci dané verze podstatnějším způsobem modifikovány. Ze strany Dodavatele budou Objednateli v dostatečném časovém předstihu před zahájením monitorování provozu poskytnuty/předány použité monitorovací nástroje (skripty) včetně doprovodné dokumentace tak, aby byl Objednatel schopen zajistit monitorování provozu i vlastními silami, a to minimálně v rozsahu prováděném Dodavatelem. Dodavateli bude umožněn přístup ke čtení produkčního prostředí KESSL, na základě tohoto práva bude možné provádět monitoring i na straně Dodavatele.

g) Zajistit bezpečnost KESSL. Při realizaci předmětu plnění musí Dodavatel garantovat zachování bezpečnosti KESSL. Objednatel požaduje, aby Dodavatel prováděl bezpečnostní testy KESSL vždy před předáním dodávky nové verze nebo hotfixu/patche KESSL, a to minimálně v rozsahu dle Přílohy číslo 06 této Smlouvy. Na základě zjištěných zranitelností nebo při jiných bezpečnostních testech, auditech, penetračních testech anebo na základě zjištění výskytu možné zranitelnosti musí Dodavatel zajistit včasný návrh a realizaci opatření schválených Objednatelem. Objednatel požaduje, aby k minimalizaci rizik spojených s možnými chybami při vývoji externích aplikací Dodavatel při vývoji používal nástroj pro kontrolu bezpečnosti např. Netsparker, Burp suite professional, Acunetix, Metasploit, Nessus. Při realizaci předmětu plnění musí Dodavatel minimálně zajistit splnění požadavků kladených na informační systémy veřejné správy a významné informační systémy dle platných právních předpisů. Dodavatel se zavazuje plnit Pravidla pro dodavatele - minimální bezpečnostní standard pro významné dodavatele, který je uveden v Příloze číslo 07 této Smlouvy.

h) Zajistit vytvoření a poskytovat součinnost při správě projektové dokumentace dle závazných právních předpisů zejména ve formě předávání všech podkladů souvisejících s projektem v rozsahu daném těmito předpisy.

3 Podmínky poskytování Služeb na objednávku

1. V rámci předmětu plnění této Smlouvy budou poskytovány další služby související s KESSL v celkovém maximálním rozsahu 450 ČLD (člověkodnů).

2. Služby na objednávku zahrnují zejména:

    a) rozvoj KESSL nad rámec poskytování update a upgrade aplikací KESSL vzniklých samostatnou, inovační činností Dodavatele, a to včetně změn vyvolaných legislativními požadavky vyplývajících z nařízení EU, zákonů a vyhlášek, které jsou pro vedení spisové služby státní správy nezbytné;

    b) údržbu KESSL nad rámec vyhrazených 7 ČLD měsíčně nebo v období po uplynutí prvních 36 měsíců účinnosti Smlouvy;

c) podporu při řešení havárií KESSL způsobené externím vlivem (např. havárie na infrastruktuře);
d) řešení chyb ostatních komponent KESSL, včetně SW;
e) podporu provozu KESSL případně podporu při instalacích nad rámec poskytnutý v rámci Servisní podpory a provozní údržby;
f) součinnost při řízení životního cyklu SW;
g) vypracování závazných technických podmínek pro obstarání technologické infrastruktury;
h) mimořádné konzultace mimo běžný rámec podpory provozu a mimo řešení rozvojových požadavků, které jsou zpracovávány do konkrétních verzí KESSL;
i) prezentace změn obsažených v aktuální dodávce;
j) aktualizaci bezpečnostní dokumentace;
k) vytvoření exit plánu;
l) školení.

3. Služby na objednávku budou Dodavatelem realizovány (poskytovány) na základě Objednávky Objednatele. Dodavatel se zavazuje poskytnout v případě potřeby své personální kapacity pro tyto požadavky v minimálním objemu 10 ČLD měsíčně, pokud se obě strany nedohodnou jinak.

4. Konkrétní poptávka na dílčí Plnění musí být zaznamenána v HD Objednatele i Dodavatele. Dodavatel na základě poptávky založené v HD navrhne maximální počet ČLD, které potřebuje ke splnění poptávky. Dodavatel nezahájí plnění dle poptávky, pokud Objednatel na jejím základě nevyhotoví Objednávku dílčího Plnění, ve které odsouhlasí i maximální počet ČLD a stanoví požadovaný termín dokončení dílčího Plnění. Objednávka musí být podepsána Zástupcem Objednatele na úrovni oprávněné osoby. Objednávka musí být potvrzena podpisem Zástupce Dodavatele na úrovni oprávněné osoby.

5. Počet ČLD vyhrazený pro splnění Objednávky lze překročit jen písemnou změnou ve formě dodatku Objednávky (opět podepsané Zástupcem Objednatele na úrovni oprávněné osoby) na základě prokazatelného důvodu, který Dodavatel v době nacenění nemohl předpokládat. Objednávky a změny Objednávek ve formě dodatků potvrzené oprávněnou osobou Objednatele musí být potvrzeny oprávněnou osobou Dodavatele a doručeny zpět Objednateli do 5 pracovních dní (Objednávka se stává závaznou až po zveřejnění v Registru smluv pokud její cena plnění přesahuje minimální částku pro publikování v Registru smluv, pokud Objednávka nepodléhá zveřejnění v Registru smluv, stává se závaznou již po doručení s potvrzením Dodavatele Objednavateli). Dodavatel postupuje v realizaci potvrzené Objednávky tak, aby příslušné dílčí Plnění předal Objednateli k akceptaci v termínu stanoveném Objednatelem v Objednávce, případně v dodatku k Objednávce.

6. Celkový objem 450 ČLD nemusí být Objednatelem vyčerpán, tj. Objednatel není povinen odebrat služby v celém předpokládaném objemu.

4 Licenční ujednání

1. Součástí Plnění může být Plnění, které naplňuje znaky díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“). V této souvislosti pak poskytuje Dodavatel Objednateli výhradní oprávnění k výkonu práva autorské dílo užít (dále jen „licenci“), a to včetně případných zdrojových kódů, všemi známými způsoby pro území celého světa a na celou dobu trvání majetkových autorských práv. Licence je poskytována jako výhradní, Objednatel je oprávněn do autorského díla zasahovat resp. autorské dílo měnit. Objednatel není povinen licenci využít.

2. Dodavatel je povinen zajistit pro Objednatele licenci takovým způsobem, aby mohl být naplněn účel této Smlouvy a byla dodržena všechna licenční ujednání k dílu a všechny právní předpisy upravující jeho užití, a to alespoň v rozsahu nezbytném pro naplnění účelu Smlouvy.

3. Dodavatel prohlašuje, že vlastní právně nezbytná oprávnění k dílu, zejména, nikoliv však výlučně, že disponuje majetkovými právy k dílu, resp. oprávněním k jejich výkonu a je oprávněn je poskytnout v potřebném rozsahu Objednateli, a to včetně příslušných oprávnění v potřebném rozsahu, které vztahují k platformě abcSuite, na jejímž základě KESSL funguje (mimo jiné tedy např. uzavřel či uzavře pracovní či jiné smlouvy, na základě kterých se stane vykonavatelem majetkových práv autorských k dílu s právem postoupení práva výkonu majetkových práv autorských).

4. Dodavatel prohlašuje, že užitím díla Objednatelem nebudou neoprávněně porušena žádná práva a oprávněné zájmy třetích osob, kromě práv duševního vlastnictví také např. právo na ochranu osobnosti fyzických osob a právo na ochranu dobré pověsti právnických osob.

5. Dodavatel se zavazuje, že jakákoli dodaná nebo zpřístupněná aktualizace, nebo jiná úprava je autorskoprávně nezávadná dle této Smlouvy a podléhá stejné licenci, jako je uvedená v této Smlouvě.

6. Dodavatel se zavazuje zajistit služby podpory (maintenance) k licencím v dostatečné rozsahu, je-li to pro naplnění účelu Smlouvy nezbytné, resp. vyžadují-li to licenční či jiné podmínky použití tohoto SW.

7. Odměna za veškerá oprávnění poskytnutá Objednateli dle této Smlouvy je již zahrnuta v ceně Plnění dle této Smlouvy. Cena Plnění obsahuje všechny licenční odměny, které mohou při Plnění z této Smlouvy vzniknout. Dodavatel není oprávněn uplatňovat další licenční poplatky s ohledem na způsob použití licencí a charakteristiku prostředí, ve kterém jsou užívány. V ceně Plnění dle této Smlouvy je zahrnuta i cena případně poskytnutých služeb podpory k SW, či jiných souvisejících Plnění, se kterými jsou spojeny jednorázové či pravidelné poplatky, za celou dobu trvání Smlouvy. Smluvní strany mají za to, že je tímto odměna za licence ujednána, resp. je sjednán způsob jejího určení dostatečným způsobem s ohledem na ustanovení § 2366 občanského zákoníku.

8. Dodavatel touto Smlouvou poskytuje Objednateli licenci k dílu, přičemž účinnost této licence nastává okamžikem podepsání akceptačního protokolu s výsledkem „akceptováno“; do té doby je Objednatel oprávněn dílo užít v rozsahu a způsobem nezbytným k naplnění účelu této Smlouvy.

5 Doba a místo Plnění

1. Tato smlouva je uzavřena na dobu určitou v délce trvání od 48 měsíců od prvního dne měsíce následujícího po účinnosti Smlouvy, nejdříve však od 1. 1. 2024. Služby Servisní podpory a provozní údržby budou poskytovány po dobu prvních 36 měsíců účinnosti Smlouvy. Služby na objednávku budou poskytovány po celou dobu účinnosti Smlouvy.
2. Místem Plnění této Smlouvy je sídlo Dodavatele (v případě vzdálených zásahů), sídlo Objednatele (nelze-li řešit vzdáleným zásahem), případně jiné místo určené Objednatelem v souladu s touto Smlouvou, jejími dodatky nebo podle jiné prokazatelné dohody smluvních stran. Objednatel umožní Dodavateli vstup na místo provádění Plnění, vyžaduje-li to Plnění této Smlouvy.
3. Chce-li Objednatel změnit místo, kde je instalováno podporované programové vybavení, je povinen v dostatečné lhůtě předem s Dodavatelem tuto změnu projednat a po dohodě s ním zajistit potřebné technicko-organizační podmínky pro pokračování poskytování Plnění Dodavatelem. Změna podmínek bude stvrzena dodatkem této Smlouvy podepsaným oběma smluvními stranami.
4. Pokud se obě strany dohodnou, Dodavatel může poskytovat Plnění podle této Smlouvy i prostřednictvím vzdáleného připojení.

6 Komunikace, oprávněné osoby a jejich zástupci, součinnost

1. Veškerá komunikace Objednatele s Dodavatelem v průběhu Plnění Smlouvy bude probíhat v českém nebo slovenském jazyce.
2. Každá strana tímto jmenuje své zástupce ve věcech Plnění této Smlouvy. Zástupci smluvních stran (též jen „**Zástupci smluvních stran**“ nebo „**Zástupci stran**“) budou zodpovídat za reprezentaci příslušné smluvní strany v technických a provozních záležitostech. Míra oprávnění se snižuje od horních řádků směrem ke spodním. Zadávat a potvrzovat Objednávky či jejich změny (dodatky) jménem Objednatele i Dodavatele je oprávněna pouze osoba Zástupce uvedená na prvním řádku jako „oprávněná osoba“.

3. Každá ze smluvních stran jmenuje následující oprávněnou osobu a její zástupce:

Dodavatel

	Jméno a příjmení	Kontaktní údaje
Oprávněná osoba	[redacted]	[redacted]
Zástupce oprávněné osoby	[redacted]	[redacted]
Zástupce – Ředitel projektu	[redacted]	[redacted]
Zástupce – Vedoucí projektu	[redacted]	[redacted]

Objednatel

	Jméno a příjmení	Kontaktní údaje
Oprávněná osoba	[redacted]	[redacted]
Zástupce oprávněné osoby	[redacted]	[redacted]
Zástupce – Ředitel projektu	[redacted]	[redacted]
Zástupce – Vedoucí projektu	[redacted]	[redacted]

4. Smluvní strany jsou oprávněny jednostranně změnit výše uvedené osoby, jsou však povinny na takovou změnu druhou stranu písemně předem upozornit.

5. Není-li pro konkrétní případ sjednáno jinak, veškerá oznámení, která vyplývají z této Smlouvy, budou mít písemnou, nebo elektronickou formu a budou druhé straně doručeny jednou z následujících možností – datová schránka Objednatele/Dodavatele, elektronická pošta (e-mail podatelny Objednatele/kontaktní e-mail Dodavatele), doporučená poštovní zásilka, nebo osobně předáním proti podpisu Zástupci druhé smluvní strany.

6. V případě nedohody na VV je problém či spor eskalován na úroveň ŘV. Pokud nedojde k vyřešení sporu či problému na úrovni ŘV, je dalším eskalačním jednáním jednání oprávněných osob Objednatele i Dodavatele, které mohou předložit návrh řešení problému či sporu následujícímu ŘV. Pokud ani po takovém procesu nedojde ke shodě a některá ze stran požaduje dořešení problému či sporu, bude tento předložen k řešení příslušnému soudu.

7. Smluvní strany se zavazují úzce spolupracovat, zejména si poskytovat úplné, pravdivé, včasné informace a dohodnuté podmínky a součinnost umožňující řádné Plnění Smlouvy.

8. V zájmu plnění Smlouvy jsou smluvní strany povinny plnit řádně a včas své závazky tak, aby nedocházelo k prodlení s jejich plněním.

9. Objednatel zajistí konzultace k vyjasnění obsahu předmětu Plnění s věcně příslušnými pracovníky Objednatele v termínu a rozsahu dohodnutému Zástupci obou stran.

10. Dodavatel garantuje, že bude aktivně spolupracovat či poskytne součinnost dodavatelům a výrobcům stávající technologické infrastruktury, programového vybavení a souvisejících či spolupracujících interních či externích aplikací či informačních systémů.

11. Objednatel poskytne Dodavateli přiměřenou a účinnou součinnost. Tato součinnost mimo jiné zahrnuje poskytování informací potřebných pro identifikaci příčin vad, zajištění přístupu k technickému vybavení a programovým prostředkům souvisejícím s provozem aplikací KESSL, případně dalších požadavků na infrastrukturu, které budou Objednateli specifikovány.

12. Objednatel zajistí potřebné technicko-organizační podmínky vyplývající z povahy předmětu Plnění podle této Smlouvy a dohodnuté oprávněnými osobami obou stran, což zahrnuje:
    a) zajištění fyzického a síťového přístupu (v případě dohody obou stran o vzdáleném přístupu) do datových center ve všech lokalitách pro určené pracovníky Dodavatele,
    b) zajištění fyzické bezpečnosti instalované HW technologie proti přístupu nepovolaných osob,
    c) údržbu a administraci funkčnosti HW a OS,
    d) při řešení nestandardních stavů aplikací KESSL a/nebo EPVDS, je předpokládána funkční vrstva Oracle DB a Oracle iAS, HW, OS a sítě.

7 Akceptační řízení

1. Do 15 dnů od nasazení Plnění na produkční prostředí Dodavatel Objednateli předloží akceptační protokol, který Objednatel nejpozději do 15 dnů od převzetí buď písemně potvrdí, nebo sdělí Dodavateli písemně výhrady k předávanému plnění s vyznačením jejich závažností. Dodavatel vyhodnotí do 5 pracovních dnů vznesené výhrady a předloží Objednateli své vyjádření k připomínkám. Za oprávněné výhrady se budou považovat takové, které poukazují na nedostatky Plnění, jež jsou v rozporu se Smlouvou a/nebo dílčími Objednávkami, zejm. se specifikací uvedenou v zadání změnového požadavku v HD Objednatele i Dodavatele, případně v dalších oboustranně schválených dokumentech. Pokud Dodavatel s výsledným vyhodnocením výhrad nesouhlasí, požádá písemně do 5 pracovních dnů od předání vyhodnocení Objednatele o zahájení jednání na úrovni Zástupců stran o způsobu řešení a vypořádání sporných výhrad. Výsledky tohoto řízení budou uvedeny do akceptačního protokolu. Pro vyloučení pochybností se uvádí, že nemůže dojít k fikci akceptace bez výhrad; akceptaci bez výhrad musí vždy potvrdit výslovně Objednatel.

2. Předmět Plnění se považuje za předaný, potvrdí-li Objednatel podpisem v akceptačním protokolu, že předmět Plnění přebírá bez výhrad, případně s výhradami (viz níže).

3. Možné výsledky akceptačního řízení

   - *Akceptováno*

   V případě, že Objednatel v průběhu akceptačního řízení nenalezne v předaném Plnění žádné vady ani nedodělky, uvede Objednatel do akceptačního protokolu, že předané plnění přebírá bez výhrad a obě strany akceptační protokol potvrdí podpisem Zástupce Objednatele.

   V případě akceptace je Dodavatel oprávněn fakturovat cenu Plnění.

   - *Akceptováno s výhradou*

   V případě, že budou v průběhu akceptačního řízení stanoveny v předávaném Plnění vady nebo nedodělky, nebránící zásadně dalšímu užití Plnění, dohodnou se Objednatel a Dodavatel na termínu, do kterého Dodavatel tyto vady a nedodělky odstraní. Nedohodnou-li strany tento termín, pak platí, že Dodavatel odstraní vady/nedodělky do 5 pracovních dnů. Objednatel do akceptačního protokolu uvede seznam vad/nedodělků s termíny jejich odstranění. V akceptačním protokolu se uvede, že předávané Plnění bylo akceptováno s výhradami a obě strany akceptační protokol potvrdí podpisem Zástupců stran. Pokud Dodavatel nebude schopen vady/nedodělky, uvedené v akceptačním protokolu, odstranit v dohodnutém termínu, je povinen poskytnout Objednateli slevu z ceny ve výši 0,5 % z celkové ceny předávaného Plnění bez DPH za každý i započatý den prodlení od původního data uvedeného v Objednávce popřípadě v Dodatku objednávky.

   - *Neakceptováno*

   V případě, že budou v průběhu akceptačního řízení v předaném Plnění zjištěny vady a nedodělky, které by bránily v užití Plnění či jeho části, respektive Plnění neodpovídá podmínkám nezbytným pro akceptaci uvedeným výše, není předané Plnění akceptováno. Obě strany se dohodnou na termínech nového předání a nového akceptačního řízení. Do akceptačního protokolu Objednatel uvede, že předané plnění nebylo akceptováno, popíše vady a nedodělky, případně požadavky na dopracování, termíny nového předání a akceptačního řízení a obě strany akceptační protokol potvrdí svým podpisem. V tomto případě je Dodavatel v prodlení s předáním Plnění a Objednatel uplatní sankce z prodlení. Doba prodlení s plněním se přitom počítá od smluvního termínu splnění (případná nesoučinnost Objednatele se do doby prodlení Dodavatele nezapočítává). Při neakceptaci předmětu Plnění nevzniká Dodavateli právo fakturovat.

4. Vlastnické právo k hmotným součástem Plnění přechází na Objednatele podepsáním akceptačního protokolu s výsledkem „akceptováno“. Pokud je akceptační řízení ukončeno akceptací s výhradou, tak vlastnictví přejde až po odstranění vad. Nebezpečí škody na hmotných součástech Plnění (či jeho dílčí části) přejde z Dodavatele na Objednatele dnem protokolárního převzetí hmotných součástí Plnění (či jeho dílčí části) a Objednateli zároveň vznikne právo hmotné součásti Plnění (či jeho dílčí části) užívat v souladu s účelem této Smlouvy.

8 Platební podmínky

1. Celková cena služeb činí celkem 9 180 000,- Kč bez DPH tj. 11 107 800,- Kč včetně 21 % DPH a je členěna takto:

Číslo položky	Předmět Plnění	Jednotka	Počet jednotek	Cena za jednotku v Kč bez DPH	Celková cena v Kč bez DPH	Celková cena v Kč včetně DPH
1	Servisní podpora a provozní údržba	*Kalendářní měsíc*	*36*	120 000,-	4 320 000,-	5 227 200,-
2	Služby na objednávku	*ČLD*	*450*	10 800,-	4 860 000,-	5 880 600,-
3	Celková cena Plnění	-	-	-	9 180 000,-	11 107 800,-

2. Cena Plnění zahrnuje veškeré náklady Dodavatele nutné k poskytnutí Plnění, jakož i veškeré náklady související (např. cestovní náhrady, náklady na ubytování, náklady na přepravu a čas strávený na cestě, to vše na území hlavního města Prahy). Dodavatel prohlašuje, že před podpisem této Smlouvy, důkladně prošel zadávací dokumentaci, zvážil všechny varianty možného způsobu Plnění zakázky a na základě těchto informací stanovil cenu Plnění uvedenou do nabídky. Tato cena je maximální a nepřekročitelná (s výjimkou změny sazby DPH) a Dodavatel je povinen za tuto cenu Plnění dokončit tak, aby bylo dosaženo účelu a předmětu této Smlouvy, a to i v případě, že by se v průběhu Plnění Smlouvy zjistilo, že ke splnění účelu a předmětu této Smlouvy je nutné vynaložit další náklady nebo zvolit jiné postupy. Pokud Dodavatel v rámci Plnění předmětu Smlouvy vykoná cesty mimo území hlavního města Prahy, je Dodavatel po předchozím vzájemném odsouhlasení oprávněn Objednateli vyúčtovat cestovní náhrady a náklady dle platných směrnic MF.

3. Smluvní strany se dohodly na bezhotovostním placení na účet Dodavatele dle pravidel uvedených v této Smlouvě.

4. Dodavatel provede fakturaci ceny za Servisní podporu a provozní údržbu vždy po konci čtvrtletí. Cena za Služby na objednávku bude fakturována podle skutečně akceptovaných dílčích Plnění (Akceptace musí být bez výhrad). Cena Plnění může být snížena o slevu z ceny za nedodržení podmínek Smlouvy.

5. Vystavená faktura bude mít náležitosti stanovené zákonem o DPH č. 235/2004 Sb., v platném znění a termín splatnosti 21 dnů po doručení Objednateli. Povinnost zaplatit je splněna dnem odepsání příslušné finanční částky z bankovního účtu Objednatele na účet Dodavatele, není-li smluvními stranami sjednáno jinak. Faktura může být zaslána do datové schránky úřadu (uuaaatg), nebo elektronicky na cuzk@cuzk.cz. Veškeré Faktury Dodavatele musí obsahovat náležitosti daňového dokladu podle příslušných právních

předpisů, zejména pak zákona o dani z přidané hodnoty, v platném znění, a zákona o účetnictví, v platném znění. V každé Faktuře Dodavatele musí být odkaz na č. j. této Smlouvy Objednatele. Přílohou faktury za Servisní podporu a provozní údržbu musí být odsouhlasené měsíční výkazy práce schválené Zástupcem Objednatele. V případě fakturace za Plnění dle Objednávky, musí být na faktuře č. j. této Smlouvy Objednatele i příslušné č. j. Objednávky Objednatele a jako příloha Faktury musí být připojen akceptační protokol Plnění dle příslušné Objednávky schválené Zástupcem Objednatele se závěrem „Akceptováno bez výhrad“. U každého akceptovaného dílčího Plnění musí být uvedeny souhrnné hodnoty počtu odpracovaných hodin, respektive ČLD vycházející z podepsaných řádných Objednávek.

6. Nebude-li vystavená faktura obsahovat náležitosti uvedené v předchozích ustanoveních nebo bude chybně vyúčtována cena, bude taková faktura do data splatnosti Dodavateli vrácena k doplnění scházejících údajů nebo k opravě nesprávných údajů. Dodavatel provede opravu vystavením nové faktury s novou dobou splatnosti, která nesmí být co do počtu dnů kratší než doba splatnosti původní faktury. Bude-li vadná faktura vrácena, přestává běžet původní doba splatnosti. V takovém případě nedojde k prodlení s placením. Celá doba splatnosti běží znovu ode dne doručení nově vystavené faktury na konkrétní fakturační místo.

9 Sankční podmínky

1. V případě prodlení Objednatele s úhradou plateb sjednaných v této Smlouvě, je Dodavatel po Objednateli oprávněn požadovat uhrazení smluvní pokuty ve výši 0,05 % z dlužné částky za každý započatý den prodlení.

2. V případě prodlení s odstraněním vad je povinen Dodavatel poskytnout slevu z ceny ve výši 1 000,-Kč bez DPH za každou i započatou hodinu prodlení v případě kritické vady a ve výši 4 000,-Kč bez DPH za každý i započatý den prodlení v případě vážné vady. Poskytnutím slevy z ceny nezaniká povinnost odstranit vady.

3. V případě prodlení s předáním Plnění dle Objednávek je povinen Dodavatel poskytnout slevu z ceny ve výši ve výši 0,5% z ceny předávaného (dílčího) Plnění bez DPH za každý i započatý den prodlení.

4. Za porušení povinnosti mlčenlivosti je porušující smluvní strana povinna uhradit druhé smluvní straně pokutu ve výši 100 000 Kč, a to za každý jednotlivý případ porušení povinnosti. Právo vymáhat a účtovat smluvní pokutu za porušení povinnosti mlčenlivosti vzniká oprávněné smluvní straně prvním dnem následujícím po doručení oznámení o prokazatelném porušení povinnosti mlčenlivosti smluvní stranou.

5. Celkově slevy uplatněné Objednatelem v součtu nepřesáhnou maximální Celkovou cenu Plnění dle Smlouvy bez DPH, případně nižší celkovou reálně hrazenou cenu, pokud Objednatel nevyčerpá celý rozsah Smlouvy.

6. Sleva z ceny bude poskytnuta v rámci fakturace bezprostředně následující po porušení povinnosti Dodavatele.

7. Poskytnutí slevy z ceny či smluvní pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky.

8. Každá ze smluvních stran je oprávněna požadovat náhradu škody i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje sleva z ceny či smluvní pokuta, a to v celém rozsahu. Odstoupením od smlouvy nárok na slevu z ceny či smluvní pokutu nezaniká.

10 Povinnost mlčenlivosti

1. Za důvěrné informace se bez ohledu na formu jejich zachycení považují ty informace, které jedna ze smluvních stran výslovně označila za důvěrné (dále jen „Důvěrné informace“).

2. Objednatel považuje mimo jiné za důvěrné veškeré technické informace o jeho vnitřním prostředí a technické detaily týkající se technické infrastruktury, které nejsou obecně známé.

3. Smluvní strany se zavazují, že během Plnění Smlouvy i po jejím ukončení budou chránit Důvěrné informace druhé smluvní strany, o kterých se dozví od druhé smluvní strany v souvislosti s Plněním Smlouvy, tak, jako chrání svoje vlastní informace stejné důležitosti a budou ve vztahu k nim zachovávat mlčenlivost a nezpřístupní je třetí osobě. Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na Plnění této Smlouvy, o povinnosti mlčenlivosti a ochrany Důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na Plnění této Smlouvy.

4. Za třetí osoby se ve smyslu této Smlouvy nepovažují:
   a) zaměstnanci smluvních stran a osoby v obdobném postavení,
   b) poddodavatelé druhé smluvní strany za předpokladu, že se podílejí na Plnění této Smlouvy nebo na Plnění spojeném s Plněním dle této Smlouvy, Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této Smlouvě.

5. Bez ohledu na výše uvedená ustanovení se za Důvěrné informace nepovažují informace, které:
   a) se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení povinnosti druhé smluvní strany či právních předpisů;
   b) měla druhá smluvní strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy;
   c) po podpisu této Smlouvy poskytne druhé smluvní straně třetí osoba, jež není omezena v takovém nakládání s informacemi;
   d) je-li zpřístupnění informace vyžadováno zákonem či jiným právním předpisem včetně práva EU nebo závazným rozhodnutím oprávněného orgánu veřejné moci;

e) jsou obsažené ve Smlouvě (ledaže podléhají výjimce z uveřejnění podle příslušných právních předpisů) anebo jsou zveřejněné na příslušných webových stránkách dle platné právní úpravy;
f) které jsou poskytnuty se souhlasem druhé smluvní strany.

6. Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající smluvní strany a přijímající smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní Důvěrné informace. S výjimkou rozsahu, který je nezbytný pro Plnění této Smlouvy, se obě smluvní strany zavazují neduplikovat žádným způsobem Důvěrné informace druhé smluvní strany, nepředat je třetí osobě ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Smluvní strany se zároveň zavazují nepoužít Důvěrné informace druhé smluvní strany jinak než za účelem Plnění této Smlouvy.

7. Veškerá data a provozní údaje zůstávají výhradním vlastnictvím Objednatele, Dodavatel je s nimi oprávněn nakládat pouze v nezbytně nutném rozsahu, tj. neduplikovat je žádným způsobem, nepředat je třetí osobě ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu, a to pouze po nezbytně dlouhou dobu. Veškerá data, provozní údaje, přihlašovací údaje apod. musí být Dodavatelem zlikvidována nejpozději s ukončením Smlouvy.

11 Podmínky poskytování záruky za jakost / záruky na funkčnost SW (společně dále „záruka“)

1. Dodavatel poskytuje na Plnění dle Smlouvy záruku za jakost (funkčnost) Plnění v délce 24 měsíců ode dne nasazení změny/úpravy/verze na produkční prostředí Objednatele, zároveň však nejdéle do uplynutí 36 měsíců od začátku účinnosti Smlouvy.

2. Počátek běhu záruční doby je stanoven na den následující po dni podepsání akceptačního protokolu s výsledkem „akceptováno“. Pokud je akceptační řízení ukončeno akceptací s výhradou, tak doba záruky počíná běžet až po odstranění vad.

3. Vyskytne-li se vada/problém, u níž nelze jednoznačně určit, která strana je odpovědná za její odstranění, vyvine Dodavatel v součinnosti s Objednatelem veškeré úsilí a učiní odpovídající opatření s cílem identifikovat příčinu vady a určit způsob jejího odstranění.

4. Poskytnutá záruka se vztahuje na všechny části Plnění, včetně příslušenství.

5. Záruka se vztahuje na funkčnost Plnění, jakož i na vlastnosti požadované Objednatelem.

6. Záruka se prodlužuje o dobu, po kterou mělo Plnění vadu bránící jeho řádnému užívání Objednatelem.

7. Veškeré zjištěné nedostatky, nedodělky a vady Plnění, které se vyskytnou v záruční době, je Dodavatel povinen odstranit na své náklady v termínech uvedených níže po jejich oznámení Objednatelem. Pokud se bude jednat o požadavek spadající do průběžné

údržby se stupněm závažnosti 1 (kritická vada), bude řešen dle příslušné SLA také na náklady Dodavatele.

8. Dodavatel musí vždy provést řádnou identifikaci požadavku, včetně návrhu základního způsobu řešení bez ohledu na to, zda se jedná o vadu systému KESSL, HW, souvisejícího SW nebo jinou vadu. Ukáže-li se však později, že provedená identifikace a kategorizace vady byla ze strany Dodavatele chybná, a o vadu KESSL se jednalo, počítá se SLA a případné sankce za její nedodržení od původního okamžiku nahlášení.

9. Pokud se nebude jednat o chybu KESSL spadající do záručního servisu, ale bude se jednat o chybu KESSL, a toto zjištění bude oboustranně odsouhlaseno, bude požadavek dále řešen buď v rámci provozní údržby, případně v rámci Služeb na objednávku.

10. Dodavatel odpovídá Objednateli za případnou škodu, která mu vznikne z titulu neodstranění vady díla ve sjednaném termínu.

11. Pro případy, kdy odstranění vady není ve sjednané lhůtě objektivně možné, navrhne Dodavatel Objednateli náhradní řešení, které bude co nejvíce eliminovat případnou škodu Objednatele.

12. Pokud Dodavatel v KESSL využije nekomerční (Open Source) SW, vztahuje se záruka i na něj.

13. Objednatel požaduje, aby v rámci záručního servisu Dodavatel prováděl:
    a) odstraňování vad KESSL modifikovaného v rámci plnění dle této Smlouvy a kritických vad bez omezení,
    b) konfigurační řízení pro odstraňování identifikovaných vad, zejména verzování, přípravu instalačních zdrojů.

14. Dodavatel zajistí komunikaci v českém, případně slovenském jazyce.

15. Objednatel je oprávněn k hlášení závad v době Dostupnosti Služby, tj. v pracovní dny ČR od 08:00 do 16:00 hodin.
16. Doba pro odstranění vady se automaticky prodlužuje o dobu, po kterou nebyla poskytnuta součinnost za strany Objednatele (nepřítomnost administrátora na pracovišti, neumožnění přístupu k zařízení, neprovedení požadovaných testů, nedoplnění potřebných informací, nedostupnost testovacího prostředí,…).
17. Záruční vady, které budou Objednatelem nahlášeny před ukončením doby poskytování záručního servisu dle Smlouvy, je Dodavatel povinen odstranit v níže požadovaných dobách, a to i za předpokladu, že požadovaná doba vyřešení uplyne a s ohledem na okamžik jejich nahlášení až po skončení záruční doby.

18. Proces odstraňování vad/SLA (pojem „vada“ zahrnuje i incident či obdobný problém) systému KESSL bude probíhat ve třech režimech:

    a) Kritické vady (vady zabraňující provozu), tj. vady vylučující užívání KESSL nebo jeho důležité a ucelené části jako např. nefunkční komunikace s ISKN, s DMS, s EIS, s exchangovým klientem podatelen, s ISDS (odeslání, příjem a ověření dostupnosti

datové schránky pro příslušnou osobu), s IK MPSV, s RS, nedostupné dokumenty, nefunkční ověřování kvalifikovaných elektronických podpisů, pečetí a elektronických časových razítek apod. Dále pokud systém KESSL vykazuje sníženou výkonnost, tj. průměrná doba vybavení detailu záznamu s jeho atributy (metadaty) v rámci jedné hodiny přesahuje 10 sekund. Za kritickou vadu se považují také případy, kdy závažná vada spočívající ve snížené výkonnosti KESSL přetrvává déle než 3 pracovní dny. Při kritické vadě může dojít k nekonzistencím v datech.

i. Nejpozději do 4 pracovních hodin (od nahlášení, pokud proběhlo v době Dostupnosti Služby, popřípadě od začátku Dostupnosti Služby, pokud nahlášení provedl Objednatel mimo Dostupnost služby) zahájí Dodavatel práce na zjištění příčin, které vadu způsobují. O této skutečnosti Dodavatel informuje na emailovou adresu vyhrazenou pro tento účel.

ii. Jde-li o oprávněnou reklamaci, stanoví Dodavatel způsob odstranění vady a navrhne termín, do kterého bude vada odstraněna, a to i způsobem dočasného provizorního řešení, umožňujícího provoz KESSL (vzniká tak vážná vada a její odstranění se dále řídí ustanoveními této Smlouvy níže). Termín trvalého či dočasného řešení nesmí být za předpokladu funkční vrstvy Oracle DB a Oracle iAS, HW, OS a sítě delší než 8 pracovních hodin (od hlášení Objednatele o výskytu vady, pokud nahlášení proběhlo v době Dostupnosti Služby, popřípadě delším než 8 pracovních hodin od nejbližšího začátku Dostupnosti Služby, pokud nahlášení provedl Objednatel mimo Dostupnost Služby).

iii. Pokud se strany nedohodly jinak, musí být po celou dobu odstraňování vady k dispozici kontaktní osoba Objednatele, která zabezpečí požadovanou součinnost, a to dohodnutou formou přítomnosti na telefonu, fyzicky na dohodnutém pracovišti apod.

iv. Vady v testovacím prostředí (RP) nejsou považovány za kritické vady.

b) Vážné vady (vady zásadním způsobem omezující provoz), tj. vady způsobující problémy při užívání a provozování KESSL nebo jeho části, ale umožňující provoz v nouzovém režimu. Modul nebo jeho část je nefunkční, požadovanou činnost lze realizovat náhradním způsobem nebo modul povoluje vykonat nepovolenou činnost nebo některé funkce modulu nefungují korektně, ale základní funkčnost je zajištěna, nebo systém KESSL vykazuje sníženou výkonnost, tj. průměrná doba vybavení detailu záznamu s jeho atributy (metadaty) v rámci jedné hodiny přesahuje 5 sekund. U vážných vad nemůže dojít k nekonzistencím v datech.

i. Nejpozději do 16 hodin (od nahlášení, pokud proběhlo v době Dostupnosti Služby, popřípadě od začátku Dostupnosti Služby, pokud nahlášení provedl Objednavatel mimo Dostupnost služby) zahájí Dodavatel práce na zjištění příčin, které vadu způsobují.

ii. Jde-li o oprávněnou reklamaci, stanoví Dodavatel způsob, postup a termín odstranění této vady, a to i způsobem dočasného provizorního řešení, umožňujícího provoz aplikací KESSL.

iii. Odstranění vážné vady Dodavatel provede nejpozději do 64 hodin (od nahlášení, pokud proběhlo v době Dostupnosti Služby, popřípadě od začátku Dostupnosti Služby, pokud nahlášení provedl Objednatel mimo Dostupnost služby).

c) Nekritické vady (vady omezující provoz), tj. vady způsobující problémy při užívání a provozování KESSL nebo jeho části, ale umožňující provoz. Některé funkce KESSL pracují omezeně, případně modul nereaguje správně na chybné akce uživatele, poskytuje nesrozumitelná chybová hlášení, chyby uživatele nejsou indikovány okamžitě. U nekritických vad nemůže dojít k nekonzistencím v datech.

i. Nejpozději do 16 hodin (od nahlášení, pokud proběhlo v době Dostupnosti Služby, popřípadě od začátku Dostupnosti Služby, pokud nahlášení provedl Objednatel mimo Dostupnost služby) zahájí Dodavatel práce na zjištění příčin, které vadu způsobují.

ii. Jde-li o oprávněnou reklamaci, stanoví Dodavatel způsob, postup a termín odstranění této vady, a to i způsobem dočasného provizorního řešení, umožňujícího provoz KESSL.

iii. Odstranění vady Dodavatel provede v rámci dodávky již připravované opravy.

12 Ukončení Smlouvy

1. Tuto Smlouvu je možno předčasně ukončit následujícími způsoby a z následujících důvodů:

a) písemnou dohodou smluvních stran, jejíž součástí je i vypořádání vzájemných závazků a pohledávek;
b) odstoupením v případě podstatného porušení smluvních povinností druhou smluvní stranou:

i. Objednatel je oprávněn odstoupit od Smlouvy v případě, že Dodavatel je v prodlení s Plněním povinností podle této Smlouvy déle než 15 pracovních dní a toto prodlení není způsobeno okolnostmi vylučujícími odpovědnost.

ii. Dodavatel je oprávněn odstoupit od Smlouvy v případě, že Objednatel je přes písemné upozornění v prodlení se zajištěním součinnosti dle této Smlouvy, a toto neplnění trvá po dobu delší než 30 dní po tomto písemném upozornění, nebo je Objednatel i přes písemné upozornění v prodlení s placením Faktury/Faktur Dodavatele, a to déle než 30 dní od doručení písemného upozornění.

c) Objednatel je oprávněn odstoupit od této Smlouvy v případě významné změny kontroly Dodavatele s tím, že změnou kontroly Dodavatele se rozumí změna ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, změna vlastnictví zásadních aktiv, popřípadě změna oprávnění nakládat s těmito aktivy, využívanými Dodavatelem k Plnění Smlouvy.
d) obě smluvní strany mají právo odstoupit od Smlouvy v případě, že okolnosti vyšší moci trvají déle než 3 měsíce.
e) písemnou výpovědí Objednatele bez udání důvodu s výpovědní dobou 6 měsíců, která běží počínaje prvním dnem kalendářního měsíce následujícího po kalendářním měsíci, v němž byla výpověď druhé straně doručena, a končí posledním dnem šestého měsíce.

2. Účinky každého odstoupení od Smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této Smlouvy druhé smluvní straně. Odstoupením od Smlouvy nezaniká nárok na náhradu škody vzniklé porušením Smlouvy ani oprávněného nároku na zaplacení smluvních pokut resp. poskytnutí slev z cen.

3. Ukončením účinnosti této Smlouvy nejsou dotčena ustanovení Smlouvy o mlčenlivosti a ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy.

13 Vyšší moc

1. Žádná ze smluvních stran nebude považována za odpovědnou za nesplnění některého ustanovení této Smlouvy, budou-li příčinou nepředvídatelné, neodvratitelné a povinnou stranou nekontrolovatelné okolnosti nebo události, která způsobují, že Plnění povinností není možné nebo je krajně obtížné. Za vyšší moc se považují zejména epidemie, ozbrojené konflikty, přírodní katastrofy apod., a to pouze za podmínky, že splňují požadavky v předchozí větě (dále též jako „vyšší moc“).

2. Smluvní strana, která porušuje svou povinnost nebo která s přihlédnutím ke všem okolnostem má vědět, že poruší svou povinnost založenou touto Smlouvou, nebo která se dozví o okolnosti vyšší moci, bránící plnění povinnosti dle této Smlouvy, je povinna oznámit písemně druhé smluvní straně povahu překážky, která jí brání nebo bude bránit v plnění povinnosti, a o jejích důsledcích. Zpráva musí být podána bez zbytečného odkladu, nejpozději však do 5 pracovních dnů poté, kdy se povinná smluvní strana o překážce dověděla nebo při náležité péči mohla dovědět. Druhá smluvní strana je povinna přijetí takové zprávy bez zbytečného odkladu písemně potvrdit. Stejným způsobem musí být obeznámena druhá smluvní strana o ukončení okolností bránících splnění povinností vyplývajících z této Smlouvy.

14 Závěrečná ujednání

1. Tato Smlouva se řídí právním řádem České republiky. Vztahy mezi smluvními stranami se řídí zejména občanským zákoníkem, pokud Smlouva nestanoví jinak.
2. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných za každou smluvní stranu osobou nebo

osobami oprávněnými jednat jménem smluvních stran, a to předchozím řádném projednání Smluvními stranami.

3. Pro případy promlčení se použije úprava obsažená v občanském zákoníku.
4. Žádná ze stran není oprávněná bez souhlasu druhé strany postoupit práva či povinnosti vyplývající z této Smlouvy na třetí stranu.
5. Spory vyplývající z této Smlouvy nebo vzniklé v souvislosti s ní nebo vzniklé v souvislosti s Plněním mezi Dodavatelem a Objednatelem budou řešeny především dohodou. Pokud k dohodě nedojde, budou spory projednávány před soudy České republiky. V případě řešení sporů před soudem si smluvní strany sjednávají místní příslušnost prvoinstančního soudu podle místa Objednatele.
6. Smluvní strany berou na vědomí, že tato Smlouva podléhá povinnosti zveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) a nabývá účinnosti nejdříve dnem zveřejnění v registru smluv. Zveřejnění v registru smluv zajistí Objednatel.
7. Dodavatel bere na vědomí a souhlasí s tím, aby subjekty oprávněné podle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, provedly finanční kontrolu závazkového vztahu vyplývajícího z této Smlouvy s tím, že se Dodavatel podrobí této kontrole, a bude působit jako osoba povinná ve smyslu ustanovení § 2 písm. e) citovaného zákona.
8. Obě smluvní strany tímto prohlašují a potvrzují, že veškerá ustanovení a podmínky této Smlouvy byly dohodnuty mezi smluvními stranami svobodně, vážně a určitě, nikoliv v tísni a za nápadně nevýhodných podmínek a na důkaz toho připojují své podpisy.
9. Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami.
10. Nedílnou součástí této Smlouvy jsou přílohy:

Příloha číslo	**Název**
01	Seznam použitých pojmů a zkratek
02	Popis HD Dodavatele
03	Principy a způsob vedení dokumentace a projektové kanceláře
04	Interní testování na straně Dodavatele
05	Soulad dokumentace s požadavky ZoISVS a vyhláškou č. 529/2006 Sb.
06	Zajištění bezpečnostních testů
07	Pravidla pro dodavatele – minimální bezpečnostní standard pro významné dodavatele

Dodavatel:

Petar Petkov Stanchev

Digitálně podepsal Petar Petkov Stanchev
Datum: 2023.12.19 17:20:32 +01'00'

Petar Petkov Stanchev

Jednatel

Objednatel:

Ing. Karel Štencel

Podepsal Ing. Karel Štencel
DN: cn=Ing. Karel Štencel, c=CZ, o=ČR - Český úřad zeměměřický a katastrální, ou=100050, email=karel.stencel@cuzk.cz
Datum: 2023.12.20 16:40:00 +01'00'

Ing. Karel Štencel

místopředseda ČÚZK

Příloha č. 01 – Seznam použitých zkratek

Zkratka, pojem	Vysvětlení
AD	Active Directory
CR	Change request, požadavek na změnu/dokument popisující způsob řešení změnového požadavku
CVSS	Common Vulnerability Scoring System je bezplatný a otevřený průmyslový standard pro hodnocení závažnosti bezpečnostních zranitelností počítačových systémů.
ČR	Česká republika
ČLD	Člověkoden, tj. 8 hodin práce jedné osoby
ČSN	Chráněné označení českých technických norem
ČÚZK	Český úřad zeměměřický a katastrální
DB	databáze
DMS	Document Management System
DMVS	Digitální mapa veřejné správy
DoS	Denial of Services (odepření služby – typ útoku)
DP	Dálkový přístup, www rozhraní ISKN pro externí uživatele
DPH	Daň z přidané hodnoty
DS	Datová schránka
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, které bylo publikováno v Úředním věstníku Evropské unie dne 23. července 2014.
EIS	Ekonomický informační systém
EPVDS	Elektronická podatelna a výpravna datových schránek
EU	Evropská unie
GDPR	Obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation)
GP	Geometrický plán
GUI DMS	Webové rozhraní DMS
HD	Helpdesk
HW	Hardware
IČO	Identifikační číslo osoby
ID DS	Identifikátor datové schránky
IDM	Identity Management
IE	Internet Explorer
IEEE	Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství)
IETF	Internet Engineering Task Force (Komise techniky Internetu)
IK	Identifikátor klienta
IK MPSV	Identifikátor klienta Ministerstva práce a sociálních věcí
IS	Informační systém
ISDS	Informační systém datových schránek
ISKN	Informační systém katastru nemovitostí
ISO	International Organization for Standardization

ISP	Identifikace a specifikace požadavků
ISVS	Informační systémy veřejné správy
ISZR	Informační systém základních registrů
JAVA	Objektově orientovaný programovací jazyk
K	Serverovna ČÚZK
KESSL	Komplexní elektronická spisová služba
KESSL/EPVDS	KESSL a podsystém EPVDS
KIVS	Komunikační infrastruktura veřejné správy
KN	Katastr nemovitostí
KP	Katastrální pracoviště
KÚ	Katastrální úřad
MF	Ministerstvo financí
MPSV	Ministerstvo práce a sociálních věcí České republiky
MTOM	Message Transmission Optimization Mechanism
NBD	Next business day (Další pracovní den)
NEN	Národní elektronický nástroj
.NET	Microsoft Net Framework
NSESSS	Národní standard pro elektronické systémy spisové služby
OS	Operační systém
PBT	Plán bezpečnostního testování
PDF	Portable Document Format (Přenosný formát dokumentů)
PK	Projektová kancelář
PP	Produktová podpora
PROD	Produkční prostředí
RP	Referenční pracoviště
RS	Registr smluv
ŘPD	Ředitel projektu Dodavatele
ŘV	Řídící výbor, nejvyšší orgán řízení projektu
SDM	Service Desk Manager, systém evidence problémů / požadavků
SIP	Internetový protokol pro inicializaci relací (Session Initiation Protocol)
SK	Školení
SLA	Service Level Agreement, definice rozsahu dostupnosti služeb
SP	Servisní požadavek
SW	Software
T	Housingové centrum T-Mobile v Praze
tel.	Telefon
TI	Technologická infrastruktura
TP	Technická podpora
UX	User experience (uživatelská přívětivost)
VM	Vzdálený monitoring
VP	Vedoucí projektu
VSD2	Nástroj pro ověřování elektronických prvků dokumentu podle evropských knihoven
VV	Výkonný výbor, orgán řízení projektu
VZ	Veřejná zakázka
WS	Web Services, webové služby

WSDL	Web Services Description Language, XML popis WS
WWW	Word Wide Web
XML	eXtensible Markup Language, rozšiřitelný značkovací jazyk pro tvorbu strukturovaných dat
ZD	Zadávací dokumentace Veřejné zakázky „Poskytování servisní podpory a provozní údržby aplikací EPVDS a KESSL v letech 2024 – 2026“
ZKI	Zeměměřický a katastrální inspektorát
ZoISVS (Standard ISVS)	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů a prováděcí předpisy vydané na jeho základě
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
ZŘ	Zadávací řízení
ZÚ	Zeměměřický úřad
ZVBT	Zpráva o výsledcích bezpečnostních testů
ZZVZ	Zákon č. 134/2016 Sb., o zadávání veřejných zakázek

Příloha č. 02 – Popis HD Dodavatele

Vady, požadavky a dotazy budou evidovány a řešeny v interním helpdeskovém systému Cerberus.

Helpdeskový požadavek (ticket) může být založen alternativně buď prostřednictvím webového rozhraní pro helpdeskovou frontu ČÚZK, zpřístupněného klíčovým pracovníkům, nebo zasláním emailu na kontaktní adresu **cuzk-req@aplis.cz**.

K založenému požadavku je v systému automaticky vygenerován jednoznačný identifikátor a na předem definovanou emailovou adresu (obvykle skupinovou) je odesláno potvrzení o přijetí požadavku, s uvedením čísla, které bylo požadavku přiděleno ve formátu

[CUZK # xxxxx]: Subjekt obdrženého emailového požadavku.

Veškerou následnou komunikaci týkající se daného problému je pak nutné zasílat vždy s uvedením přiděleného čísla [CUZK # xxxxx]: v subjektu emailu.

Pro zvýšení přehlednosti a usnadnění správy požadavků je nutné v subjektu zasílaného požadavku uvádět kromě interního čísla helpdeskového systému Objednatele i stručnou charakteristiku daného požadavku. Tato charakteristika by měla být uváděna bez diakritiky.

V zaslaném hlášení o aplikační chybě systému EPVDS je pro urychlení řešení vhodné uvádět následující údaje:

1. Název aplikační instance, ve které byla chyba zjištěna (KUCBUD, KUHKRA, KUUSTL...)
2. Název podacího deníku ve kterém k chybě došlo (CBUD, STRA, TREO...)
3. Pod jakým uživatelským účtem byla chyba zjištěna
4. Evidenční číslo záznamu (ID ePodatelna) kterého se hlášení týká (plný formát ve tvaru xxxxxxxx/yyyy-<kod pracoviste>
5. V případě chyby WS číslo řízení
6. Číslo čarového kódu u zásilky pokud se jedná o zásilku
7. Popis postupu vyvolání chyby nejlépe doplněný printscreeny obrazovky

Postup řešení založeného požadavku je možné sledovat prostřednictvím emailové komunikace generované helpdeskovým systémem, případně i prostřednictvím webového rozhraní.

Příloha č. 03 – Principy a způsob vedení dokumentace a projektové kanceláře

Projektová knihovna bude umístěna ve složkové struktuře vytvořené v dokumentové části aplikace EPVDS/KESSL - ČÚZK - Projektová knihovna

Přístup k dokumentům bude řízen prostřednictvím přidělených ACL (Acces control listů)

Tento způsob vedení dokumentace projektových výstupů plně vyhovuje požadavkům uvedeným v kapitole 4.3.1. zadávací dokumentace.

- Vzdálený přístup pro zástupce Objednatele prostřednictvím sítě internet.
- Verzování dokumentů.
- Různé kategorie dokumentů z hlediska bezpečnosti (standardní, důvěrné, …) a možnost řízení přístupu k těmto kategoriím.
- Struktura s rozdělením dokumentů podle logických kategorií (zápis z jednání, žádosti o změnu, dokumentace, …).
- Automatické číslování nových dokumentů v kategoriích podle předchozího požadavku.
- Logování a audit přístupů do PK k jednotlivým dokumentům.
- Uložení různého typu dokumentů (Word, Excel, MS Project, ZIP, RAR, …).
- Možnost uložení jen dokumentů, které odpovídají předem oběma stranám (Objednatel/ Dodavatel), dle schválené jmenné konvence.
- Export PK na filesystém.

Instalační zdroje a popisy instalace budou předávány s každou změnou na FTP server Objednatele.

Pro každou novou verzi IS bude dodána aktualizovaná administrátorská dokumentace, uživatelská dokumentace a systémová příručka.

Příloha č. 04 – Metodika interní testování na straně Dodavatele

Vlastní aplikace spisové služby včetně jednotlivých dodávek a patch je podrobena několikastupňovému testování.

Ihned po vytvoření programového kódu, je tento kód prověřen programátorem. Pro specifické části aplikace jsou zde používány i unit testy, není to však pravidlem. Následují funkční testy na vývojovém prostředí a v případě úspěšného výsledku je vytvořen patch, který se aplikuje na referenční prostředí vytvořené na technologické infrastruktuře dodavatele, které svojí verzí odpovídá aktuální verzi implementované u Objednatele.

Na tomto prostředí je proveden systémový a uživatelský test, po jehož úspěšném výstupu je výsledný patch předán k implementaci na referenční prostředí Objednatele.

V rámci interního testování se používají aplikace

a) Apache Jmeter pro opakovaná dílčí testování aplikace a měření výkonnosti
b) SoapUI pro testování webových služeb

Dodavatel v současné době nevyužívá nástroje pro kontrolu bezpečnosti specifikované v článku 3.3.4. ZD. I když v současné době Dodavatel nepoužívá pro kontrolu bezpečnosti nástroje přesně specifikované v článku 3.3.4. ZD, garantuje, že při plnění této Smlouvy bude používat nástroje a postupy, které efektivně minimalizují rizika spojená s možnými chybami při vývoji externích aplikací.

EPVDS/KESSL je plně implementovaná v prostředí Objednatele, které kontroluje vstupní/ výstupní kanály do EPVDS/KESSL. Přímé vazby EPVDS/KESSL na vnější prostředí jsou pouze na IS datových schránek spravovaný Digitální a informační agenturou. Další vazby jsou pouze vnitřní, a to na agendové systémy Objednatele.

Provedení bezpečnostních testů v prostředí Objednatele bude výlučně se souhlasem a za aktivní spolupráce manažera kybernetické bezpečnosti Objednatele. Testy budou plánovány v rámci daného roku minimálně 1x. Dodavatel bude navrhovat pro vymezené případy i další bezpečnostní testy.

Dodavatel klade velký důraz na kvalitu a spolehlivost poskytovaných služeb, a to včetně testování v prostředí virtualizované infrastruktury. Toto testování je nezbytnou součástí podpory celkového systému EPVDS/KESSL.

Proces testování se skládá z několika klíčových kroků:

a) Funkční Testy na Vývojovém Prostředí: Iniciální fáze testování probíhá na vývojovém prostředí Dodavatele. Zde se provádějí funkční testy, aby byla zajištěna funkčnost připravovaných updatů nebo patchů.

b) Aplikace Patche na Testovací Prostředí: Po úspěšném absolvování funkčních testů je vytvořený patch aplikován na speciálně vytvořené testovací prostředí. Toto prostředí je postaveno na technologické infrastruktuře Objednatele a svou verzí odpovídá aktuální verzi implementované u Objednatele.

c) Systémový Test: V tomto kroku je proveden důkladný systémový test na zmíněném testovacím prostředí. Úspěšný výstup z této fáze je předpokladem pro předání patche k implementaci na referenční prostředí Objednatele.

d) Spolupráce při Testování Bezpečnosti: V případě, že Objednatel bude provádět testování nástroji pro kontrolu bezpečnosti specifikované v článku 3.3.4. ZD na testovacím (referenčním) prostředí, poskytne Dodavatel potřebnou součinnost. Cílem je zajištění bezpečnosti informací EPVDS/KESSL a zároveň zajištění dostupnosti a spolehlivosti služeb.

e) Evidování a Řešení Požadavků: Vady, požadavky a dotazy budou systematicky evidovány a řešeny v interním helpdeskovém systému Dodavatele Cerberus. Tento systém umožňuje efektivní sledování a řešení všech požadavků.

f) Komunikace s Objednatelem: Pro zajištění plynulé komunikace mezi Dodavatelem a Objednatelem bude využíváno webového rozhraní pro helpdeskovou frontu Objednatele, přístupného klíčovým pracovníkům, a také komunikace prostřednictvím emailu na adresu cuzk-req@aplis.cz.

g) Tímto způsobem je zajištěno, že veškeré testování v prostředí virtualizované infrastruktury je prováděno systematicky, efektivně a v souladu s nejvyššími standardy kvality. Postupy a procesy v této oblasti vyhovují požadavkům Objednatele a zaručují spolehlivé a bezpečné řešení pro Objednatele.

Příloha č. 05 – Soulad dokumentace s požadavky ZoISVS a vyhláškou č. 529/2006 Sb.

Dokumentace ohledně oprav a úprav aplikací u Objednatele je v souladu s požadavky ZoISVS a vyhlášky č. 529/2006 Sb. Zahrnuje podrobné popisy datových prvků a procesů, které jsou předmětem změn, čímž zajišťujeme transparentnost a srozumitelnost pro všechny zainteresované strany. Do projektové knihovny budou v souladu s požadavky ZoISVS a s vyhláškou č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy ukládány a verzovány minimálně následující dokumenty:

Výstupy vázané na verzi/patche KESSL

Dodavatel před instalací každé nové verze KESSL do prvního referenčního prostředí (REF A KESSL nebo REF B KESSL) předá Objednateli:

- výstupní protokol z interního testování funkčnosti a bezpečnosti na straně Dodavatele. Tento dokument obsahuje analýzu funkčnosti a bezpečnosti, která je provedena před každou instalací nové verzi/patche,
- odsouhlasené testovací scénáře Objednatelem ve formátu DOC (DOCX). Testovací scénáře budou předávány Dodavatelem Objednateli k průběžné revizi již při realizaci jednotlivých požadavků. Objednatel má právo na to, aby Dodavatel testovací scénáře rozšířil/upravil dle potřeby pro důkladné ověření funkčnosti požadavku.
- všechny zdrojové kódy včetně použitých nekomerčních (Open Source) SW, přičemž dokumentace zdrojových kódů musí být na takové úrovni, aby byla srozumitelná i třetí, nezúčastněné osobě. Dodavatel poskytuje kompletní sadu zdrojových kódů s dokumentací oprav a úprav aplikací EPVDS/KESSL i pro třetí strany,
- instalační příručku,
- dokumentaci webových služeb a dokumentaci všech WSDL, XML, XSD včetně podrobných komentářů jednotlivých elementů a atributů,
- dotčenou provozní dokumentaci,
- bezpečnostní dokumentaci,
- uživatelskou příručku,
- dokumentaci pro školení.

Dodavatel po instalaci každé nové verze/balíku patchů KESSL do produkčního prostředí dle této VZ předá Objednateli finalizováné výstupy z plnění potřebné pro další rozvoj a údržbu KESSL. Jedná se zejména o tyto výstupy:

- předávané zdrojové kódy ke změnám na objednávku včetně použitých nekomerčních (Open Source) SW, přičemž dokumentace zdrojových kódů musí být na takové úrovni, aby byla srozumitelná i třetí, nezúčastněné osobě,
- programátorská dokumentace,
- uživatelská příručka,
- instalační příručka,
- dokumentace webových služeb a dokumentaci všech WSDL, XML, XSD včetně podrobných komentářů jednotlivých elementů a atributů,
- dotčená (změněná) provozní dokumentace,
- systémová příručka IS,
- dokumentace pro školení.

Výstupy nevázané na dodávku KESSL

Dodavatel bude níže uvedené výstupy v průběhu plnění Smlouvy udržovat v aktuálním stavu a na vyžádání je ve lhůtě 1 měsíce Objednateli předá, s tím, že poslední předání výstupů Objednateli bude k datu ukončení smluvního vztahu, jedná se zejména o:

- popis používaných nástrojů a jejich nastavení,
- popis konfiguračního řízení,
- projektové standardy (jmenné konvence apod.),
- použité způsoby a metodiky vývoje,
- principy monitorování a aktualizace požadavků v systému pro evidenci požadavků,
- popis monitorování provozu,
- export problémů/požadavků z HD Dodavatele.

Dodavatel bude spolupracovat při zpracovávání dalších dokumentů, zejména bezpečnostní dokumentace, aby byly zajištěny všechny aspekty bezpečnosti a správy informačního systému.

Postupy a dodávky jsou navrženy tak, aby byly v souladu se standardy a očekáváními ve veřejné správě.

Příloha č. 06 – Zajištění bezpečnostních testů

1 Úvod

Tento dokument stanovuje pravidla a postupy pro provádění bezpečnostních testů v prostředí Objednatele k zajištění bezpečnostního testování KESSL (dále též „bezpečnostní testování“ nebo „bezpečnostní testy“).

Interní testování Dodavatele v oblasti bezpečnosti prováděné na technologické infrastruktuře Dodavatele není obsahem tohoto dokumentu.

Objednatel má zpracovanou obecnou metodiku pro provádění bezpečnostních testů ČÚZK-40683/2022 a dále specifický dokument pro projekt.

2 Členění zranitelností podle závažnosti

2.1 CRITICAL

Kritická, vyžaduje zpravidla okamžitý zásah nebo odstavení systému.

2.2 IMPORTANT

Důležitá, může být zdrojem budoucích potíží, je nezbytná náprava dle možností co nejdříve.

2.3 MEDIUM

Střední stupeň závažnosti, zvyšuje pravděpodobnost úspěšného útoku, zpravidla vyžaduje splnění určitých podmínek.

2.4 LOW

Nízký stupeň závažnosti, pouze mírně zvyšuje pravděpodobnost úspěšného útoku, vyžaduje splnění určitých podmínek.

2.5 INFORMATION

Informativní, nejedná se ve skutečnosti o zranitelnost, ale o informaci.

3 Pravidla a způsob provádění bezpečnostních testů

Bezpečnostní testování bude prováděno v testovacím prostředí Objednavatele a v předem stanoveném a Objednavatelem odsouhlaseném rozsahu.

Výjimky z rozsahu bezpečnostních testů jsou možné pouze po předchozím odsouhlasení Objednavatele.

3.1 Kritéria pro stanovení rozsahu bezpečnostního testování

Bezpečnostní testování může být vyvoláno následujícími faktory:

3.1.1 Příprava dodávky KESSL

Dodavatel při navrhování rozsahu bezpečnostního testu posuzuje:

- zda změna KESSL zasahuje přímo do bezpečnostních vlastností KESSL (změna je

s přímým bezpečnostním dopadem, např. zavedení nové webové služby, změna technologie), nebo zda změna má nebo může mít nepřímý bezpečnostní dopad, nebo zda může zasáhnout do bezpečnostních opatření KESSL (např. doplněný nebo změněný modul bez přímé vazby na bezpečnostní opatření),

- rozsah změn KESSL.

Závazný minimální rozsah bezpečnostních testů, v závislosti na charakteru změny vyjádřeném číslem verze dodávky KESSL, je uveden v následující tabulce.

Označení změny KESSL	**Jedná se o verzi změny (dodávky) označenou**	**Rozsah prováděných bezpečnostních testů**
Velká	X.Y (např. 3.0, 3.1, ..)	Bude vždy provedena kompletní sada bezpečnostních testů dle kapitoly Bezpečnostní testy webových aplikací a služeb tohoto dokumentu.
Malá	X.Y.Z (např. 3.0.1, 3.1.2, …)	Bude provedena kompletní sada bezpečnostních testů pouze v případě, že bude implementována alespoň jedna změna KESSL s možným přímým nebo nepřímým bezpečnostním dopadem.
Patch/hotfix	X.Y.Z.xx (např. 3.0.1.03)	Budou provedeny bezpečnostní testy vybraných a navržených testovacích scénářů pro příslušnou změnu s možným bezpečnostním dopadem, případně i další bezpečnostní testy navržené Objednavatelem nad rámec návrhu Dodavatele.
Změna bezpečnostního mechanismu		Budou provedeny bezpečnostní testy vybraných a navržených bezpečnostních testovacích scénářů pro příslušnou změnu na základě povahy této změny.
Nová hrozba		Budou provedeny bezpečnostní testy vybraných a případně nově navržených bezpečnostních testovacích scénářů pro příslušnou hrozbu na základě povahy této hrozby. Návrh dá vždy Dodavatel, Objednavatel ale může navrhnout vlastní bezpečnostní scénář.

Bezpečnostní testy začleňuje Dodavatel do harmonogramu dané dodávky KESSL.

Pokud není v období 12 měsíců plánována / dodána dodávka KESSL typu X.Y, začlení Dodavatel provedení kompletní sady bezpečnostních testů do vhodné dodávky KESSL typu X.Y.Z tak, aby odstup od minulého provedení kompletní sady bezpečnostních testů nebyl větší než 12 měsíců, případně lze po dohodě se Objednavatelem provést na v té době vhodném testovacím prostředí Objednavatele kompletní sadu bezpečnostních testů bez vazby na konkrétní dodávku KESSL.

3.1.2 Zjištění výskytu relevantní zranitelnosti v průběhu kybernetického bezpečnostního incidentu

V takovém případě je bezpečnostní testování prováděno v rozsahu nezbytném pro ověření, zda kybernetický bezpečnostní incident nebyl způsoben zranitelností.

Provedení bezpečnostních testů navrhuje Dodavatel na základě zjištěných informací; součástí návrhu je i vhodné začlenění do harmonogramů aktuálních/plánovaných dodávek KESSL.

3.1.3 Informace zjištěné při činnostech prováděných Manažerem nebo Architektem kybernetické bezpečnosti IS nebo Specialistou kybernetické bezpečnosti

Zdrojem těchto informací může být například sledování informačního servisu NÚKIB nebo security bulletinů; v takovém případě je bezpečnostní testování prováděno, pokud obsahuje komponentu, která může být na zranitelnost náchylná; účelem tohoto bezpečnostního testu je zjištění, zda KESSL danou zranitelnost obsahuje.

Provedení bezpečnostní testů navrhuje Dodavatel na základě zjištěných informací; součástí návrhu je i vhodné začlenění do harmonogramů aktuálních/plánovaných dodávek KESSL.

3.2 Pravidelné bezpečnostní testy na produkčním prostředí

Dodavatel poskytne součinnost a Objednavatel provádí na produkčním prostředí Objednavatele pravidelně minimálně 1 x za 12 měsíců sadu základních bezpečnostních testů v rozsahu bodu č. 4.

3.2.1 Pravidla provádění bezpečnostních testů

Bezpečnostní testy musí být opakovatelné a musí být prováděny neinvazivním způsobem.

Pro účely bezpečnostního testování na prostředí Objednavatele poskytne Objednavatel Dodavateli:

- testovací účet s přístupem do testovacího nebo produkčního prostředí Objednavatele, v němž bude probíhat bezpečnostní testování,
- přístup k KESSL s právy běžného externího uživatele (případně více uživatelů, podle jejich rolí),
- vzdálený přístup do interní sítě Objednavatele nebo fyzický přístup na pracoviště Objednavatele, pokud to bude pro bezpečností testování potřebné,
- možnost připojení koncového zařízení Dodavatele (testovacího notebooku nebo serveru) do testovacího prostředí Objednavatele.

Dodavatel je během provádění bezpečnostních testů povinen:

- účastnit se bezpečnostních testů dle schváleného „Plánu bezpečnostního testování“ (PBT),
- neověřovat prakticky zjištěnou zranitelnost vůči útoku „Denial of Services“ (DoS),
- neprovádět nevratné zásahy do systému (v případě úspěšného průniku),
- nepoužívat techniky „sociálního inženýrství“ (telefonáty nebo e-maily pod předstíranou identitou apod.),

- v případě zjištění závažné skutečnosti v průběhu testování (odstavení některé služby) okamžitě informovat Objednavatele.

Bezpečnostní testování provádí Dodavatel dle jím zpracovaných testovacích scénářů.

3.3 Způsob provádění bezpečnostních testů

Před zahájením bezpečnostního testování Dodavatel vyhotoví a předá Objednavateli dokument „Plán bezpečnostního testování KESSL pro dodávku X“ (PBT), který bude minimálně obsahovat:

- na základě kritérií dle bodu 3.1.1 seznam změn KESSL včetně uvedení, jak danou změnu vyhodnotil, tj. zda tato změna má/může mít nebo nemá bezpečnostní dopad,
- na základě bodu 3.1.2 popis kybernetického incidentu, který může indikovat zranitelnost,
- na základě bodu 3.1.3 popis možné zranitelnosti a odkaz na zdroj,
- navržený rozsah bezpečnostních testů, který bude proveden,
- harmonogram termínů provádění bezpečnostních testů.

PBT podléhá schválení ředitele odboru informatiky Objednatele.

Na základě schváleného PBT provede Dodavatel:

- v případě bodu 3.1.1 po úspěšném interním otestování v prostředí Dodavatele bezpečnostní testování v testovacím prostředí Objednavatele s instalovanou změnou KESSL, při zjištění kritické nebo důležité zranitelnosti (viz body 2.1 a 2.2) Dodavatel v případě zranitelnosti, která vznikla v důsledku plnění Dodavatele, zajistí odstranění příčiny/chyby způsobující tuto zranitelnost a spolupracuje pro opakované bezpečnostní testování se zaměřením na ověření odstranění zranitelnosti; o všech těchto skutečnostech bez prodlení informuje Objednavatele,
- v případě bodů 3.1.2 a 3.1.3 v testovacím prostředí Objednavatele testování s verzí KESSL shodnou jako na produkčním prostředí, při nižší závažnosti lze bezpečnostní test umožnit v rámci testování aktuálně připravované dodávky KESSL; bezpečnostní test lze po odsouhlasení Objednavatele provést v produkčním prostředí,
- v případě bodu 3.2 v produkčním prostředí Objednavatele umožní bezpečnostní testování s aktuální verzí KESSL.

Po ukončení bezpečnostního testování předkládá Dodavatel výsledný dokument o průběhu a dosažených výsledcích bezpečnostních testů s názvem „Zpráva o výsledcích bezpečnostních testů KESSL dodávky X“ (ZVBT). Tento dokument je předložen do 2 týdnů po ukončení testů, včetně vyjádření Dodavatele k nalezeným zranitelnostem, která budou přenesena do Registru zranitelností evidence testů KESSL. Nově nalezená zranitelnost musí být ve zprávě jasně odlišena od již dříve nalezené (pokud nebyla již dříve opravena a jedná se tedy o nový výskyt zranitelnosti).

V případě, že ZVBT obsahuje zjištěné zranitelnosti, Dodavatel zajistí svolání schůzky Dodavatele a Objednavatele, kde Dodavatel prezentuje svá zjištění a blíže informuje o návrhu/návrzích řešení. Na schůzce Objednavatel rozhodne o způsobu odstranění zranitelností nebo jejich eliminaci a o dalším postupu. Toto Dodavatel zaznamená do zápisu ze schůzky, který podepisuje zástupce Dodavatele a Objednavatele.

Neodstranění kritických a důležitých zranitelností nalezených při postupu dle bodu 3.1.1

a nezopakování ověření odstranění těchto zranitelností s vyhovujícím výsledkem může být důvodem k odkladu instalace příslušné dodávky KESSL do produkčního prostředí. Pokud zjištěná zranitelnost nevznikla v důsledku plnění Dodavatele, pak se odklad instalace nepovažuje za prodlevu v plnění na straně Dodavatele.

3.4 Ochrana dat v průběhu testování

Dodavatel se v průběhu realizace bezpečnostních testů řídí standardními pravidly pro zajištění důvěrnosti používaných informací, zejména pak:

- tam, kde je to možné, používá anonymizované informace,
- v případech, kdy použití anonymizovaných informací není možné (např. v rámci testování v produkčním prostředí), je povinen zajistit opatření, která znemožní jejich nekontrolovaný únik.

4 Bezpečnostní testy webových aplikací a služeb

V rámci bezpečnostních testů jsou testována rozhraní KESSL, k nimž přistupují uživatelé, jak interní z vnitřní sítě resortu, tak externí, kteří mají přístup zajištěn pomocí dálkového přístupu z vnější sítě.

Bezpečnostní testy musí obsahovat vždy otestování:

a) syntaxe všech uživatelských postupů

b) odolnosti proti známým typům útoků (XSS, CSRF, Session Steal, ClickJacking apod.),

c) zákazu používání tzv. skrytých polí pro důvěrná (citlivá) data,

d) zákazu používání přídavných identifikací uživatelských „session“ a obdobných autentizačních prostředků zakomponovaných v URL,

e) zákazu uvádění názvů souborů a adresářových cest v chybových hlášeních,

f) možností uživatelova odhlášení a automatického odhlášení po definované době jeho nečinnosti,

g) omezení pro používání Cookies na Cookies s časově omezenou platností, které jsou posílány zpět pouze stejnému serveru,

h) Java applety a případné jiné komponenty musí být podepsány důvěryhodnou certifikační autoritou,

i) komunikace aplikace s datovými zdroji v interní síti musí být autentizovaná,

j) možnost napadení DoS útokem,

k) další zranitelnosti definované tímto dokumentem (specifické zranitelnosti),.

l) testy na zranitelnosti uvedených v tabulce v kapitole č. 9 této Přílohy.

4.1 Penetrační testy

Při penetračním testu Dodavatel minimálně simuluje útok neoprávněné osoby z vnější sítě.

Penetrační testy se provádějí, z hlediska efektivity a správnosti, s částečnou znalostí testovaného cíle, tzv. „gray box“.

Cíle budou prověřovány ve dvou úrovních a to:

- identifikace a prověření známých zranitelností na úrovni standardních webových služeb serveru;
- a identifikace a prověření známých zranitelností na úrovni architektury vlastní webové aplikace.

Penetrační testy musí vždy ověřit, zda webová aplikace, resp. webová služba, neobsahuje žádnou ze všech známých zranitelností uvedených v kapitole č. 9 této Přílohy, bodu 1 tohoto dokumentu, spadajících pod OWASP TOP 10 – 2021.

Za tímto účelem jsou realizovány odpovídající testovací scénáře uvedené v kapitole č. 9 této Přílohy tohoto dokumentu.

Objednavatel připouští realizaci bezpečnostních testů níže uvedenými způsoby, přičemž jejich použití k ověření oblastí testování v kapitole č. 9 této Přílohy ponechává na Dodavateli.

4.1.1 Automatizované testy a automatizované testy s manuálním podílem

Pro automatizované testy a automatizované testy s manuálním podílem bude použit některý ze SW nástrojů. Druh aktuálně použitého SW nástroje návrhne Dodavatel v dokumentu PBT.

4.1.2 Manuální testování

Manuální testování podpoří Dodavatel v těch případech, kdy není možné využít automatizované testy nebo by použití automatizovaných testů nebylo dostatečně efektivní.

4.2 Specifické testy

Metodika OWASP obsahuje standardizované testy, tj. nezahrnuje všechny testovací scénáře zranitelností, které se mohou při vývoji informačního systému vyskytnout. Vzhledem k tomu budou dále pro zajištění bezpečného fungování KESSL prováděny též i další specifické testy.

Specifické testy budou vycházet a zohledňovat možná specifika kódu, zjištění ze sledování informačního servisu NÚKIB apod., zranitelnosti zjištěné při provozu KESSL, které se vyskytly jako bezpečnostní události nebo incidenty u nichž je nutné zajistit přijetí bezpečnostní opatření k zajištění jejich neopakovatelnosti nebo eliminaci a které vznikly v době před odpovídající aktualizací metodiky OWASP.

Seznam testovacích scénářů pro specifické testy je uveden v kapitole č. 9 této Přílohy tohoto dokumentu.

5 Předmět bezpečnostních testů KESSL

Předmětem bezpečnostních testů KESSL je:

- https://ep-p-epvds.cent.priv/

Dodavatel je vždy povinen zahrnout do návrhu testování další nové externí a interní části KESSL a dle toho aktualizovat tento dokument.

6 Testovací scénáře

Testovací scénáře musí zahrnovat následující údaje:

- název testovacího scénáře,
- ID testovacího scénáře,

- Tester – jméno
- verze systému,
- počet provedení scénáře,
- účel testu – popis, co je testem ověřováno,
- výchozí stav systému a vstupní podmínky,
- kroky testu – popis testovacích kroků a dat používaných pro testování,
- očekávané výsledky – kritéria úspěšnosti testu přiřazené ke každému z testovacích kroků.

7 Zpráva o výsledcích bezpečnostních testů

O provedení bezpečnostních testů pořizuje Zhotovitel Zprávu o výsledku bezpečnostních testů. Zpráva musí vždy obsahovat minimálně:

- Datum a čas provedení bezpečnostního testu
- Na jakém prostředí bylo testováno
- Změny aplikace, které jsou dodávány
- Seznam změn, které podléhají/nepodléhají bezpečnostním testům
- ID testovacího scénáře
- Jméno testera, který testování prováděl
- Manažerský souhrn s důležitými závěry bez technických detailů
- Technickou zprávu shrnující zjištění s technickými detaily a protokoly z testování
- Soupis zjištění
- Je-li součástí zprávy report generovaný nějakým SW nástrojem, je nutné specifikovat název a verzi nástroje, případně verzi pluginů. Zjištění musí být v celé zprávě jednotně klasifikována, přestože jsou použity různé SW nástroje, které mohou mít vlastní klasifikace

Nalezené kritické zranitelnosti (CVSS>7) oznamuje Zhotovitel garantovi aktiv KESSL neodkladně po nalezení kritické zranitelnosti.

Po ukončení bezpečnostního testování předkládá Zhotovitel finální dokument o provedení a dosažených výsledků bezpečnostních testů s názvem „Zpráva o výsledcích bezpečnostních testů KESSL dodávky X“ (ZVBT). Tento dokument je předložen do 2 týdnů vč. vyjádření Zhotovitele k nalezeným zranitelnostem, která budou přenesena do Registru zranitelností evidence testů KESSL.

8 Přechodná ustanovení

Dodavatel se zavazuje, že v případě uvolnění nové verze OWASP bude tento dokument do měsíce od vydání nové verze OWASP aktualizovat v souladu s novou verzí a upravit i odpovídající testovací scénáře a používat odpovídající postupy a druhy testů.

9 Seznamy testovaných zranitelností, testovacích scénářů a specifických zranitelností

9.1 Seznam zranitelností podle OWASP Top 10-2021: https://owasp.org/Top10/

Zranitelnost	Popis
A01:2021 Broken Access Control	Aplikace často používají skutečný název nebo klíč objektu při generování webových stránek. Aplikace ne vždy ověřuje, zda je uživatel oprávněn přistupovat k cílovému objektu. Útočník tak může neoprávněně manipulovat s těmito odkazy a přistupovat k jiným objektům (bez autorizace). Testeři můžou snadno manipulovat hodnoty parametrů k detekci takovýchto zranitelností. Analýza kódu rychle ukáže, zda povolení je řádně ověřeno.
A02:2021 CryptographicFailures	(dříve označované Sensitive Data Exposure) Nejběžnější chybou je nešifrování citlivých dat. Pokud se používá šifrování, jde o generování slabých klíčů, použití slabých šifrovacích algoritmů nebo slabé hashovací techniky pro hesla. Zranitelnosti v prohlížeči jsou velmi časté a snadno odhalitelné, ale těžko zneužitelné ve velkém měřítku.
A03:2021 Injection	Zranitelnost typu injektáže (SQL, LDAP, XPath, NoSQL dotazů;příkazů operačního systému, XML parsování, SMTP hlaviček, programových argumentů, atd.) je velmi běžnou chybou webových aplikací, které nastává, pokud jsou přes neošetřený vstup uživatelem poskytnutá nedůvěryhodná data poslána do překladače jako část příkazu nebo dotazu. Např. u „SQL injection“ jde o vykonání vlastního, pozměněného SQL dotazu za účelem neoprávněného přístupu k informacím, jejich změně nebo i ovládnutí daného zařízení. Zranitelnosti typu injektáže lze snadno zjistit při revizi kódu, ale těžší je zjišťovat jejich přítomnost pomocí testů vzhledem k velké variabilitě manipulace parametrů http dotazů.
A4:2021 Insecure Design (nová)	Nejistý design je zaměřen na rizika spojená s konstrukčními nedostatky. Kontrola bezpečných vzorů a principů návrhu vč. referenční architektury.
A5:2021 Security Misconfiguration	Bezpečnostně chybná konfigurace může nastat na jakékoliv úrovni infomačního systému ať už to je webový server, aplikační server, databáze, framework, atd. Vývojáři a systémoví administrátoři musí úzce spolupracovat, aby zajistili, že konfigurace všech částí infomačního

Zranitelnost	Popis
	systému.
A6:2021 Vunerable and Outdated Components	(dříve označované jako Using Components with Known Vunerabilities) Prakticky každá aplikace má problémy s použitím komponent (knihovny, frameworky a další softwarové moduly) obsahujících známé zranitelnosti, protože většina vývojářů se nesoustředí na zajištění aktualizací komponenty/knihoven. V mnoha případech vývojáři ani neznají, jaké všechny komponenty se používají, natož jejich verze. Závislosti komponent situaci ještě zhoršují. Detekce se provádí zpravidla lokálně v rámci zdrojového kódu, ale částečně ji lze provést i pomocí penetračního testu.
A7:2021 Identification and Authentication Failures	(dříve označované jako BrokenAuthetication) Vývojáři často vytváří autentizační mechanismy a řízení relací, ale jejich správné vytvoření není jednoduché. Jako výsledek těchto snah bývají často zranitelnosti v oblastech odhlášení, správy hesel, dlouhé časové limity pro relace, aktualizace účtů atd. Útočníci mohou kompromitovat hesla, klíče nebo autentizační identifikátory k předstírání jiných uživatelských identit. Nalezení těchto zranitelností může být občas těžké, protože každá takováto implementace bývá jedinečná.
A8:2021 Softwarea and Data Integrity Failures (nová)	Kategorie se zaměřuje na vytváření předpoklad souvisejících s aktualizacemi softwaru, důležitými daty a kanály CI/CD bez ověření integrity. Jeden z nejvíce vážených dopadů dat CommonVunerability and Exposures/Common Vunerability Scoring System (CVE CVSS) mapovaných na 10 CWE v kategorii A8:2017 Insecure Deserialization je nyní součástí této větší kategorie
A9:2021 SecurityLogging and Monitoring Failures	(dříve označované jako Insufficient Logging& Monitoring) Jedna z možných strategií pro zjištění, zda je správně nastaven monitoring a logování, je prověřit protokoly po penetračním testování. Činnosti testerů by měly být dostatečně zaznamenány, aby bylo možné zjistit, jaké škody by mohly být způsobeny. Nejúspěšnější útoky začínají zkoumáním zranitelnosti. Povolení pokračování takových zkoumání může zvýšit pravděpodobnost úspěšného útoku téměř na 100%.
A10:2021:ServerSideRequestForgery (SSRF) (nová)	Úspěšný útok SSRF může často vést k neoprávněným akcím nebo přístupu k datům v rámci organizace, ať už v samotné zranitelné aplikaci nebo v jiných back-endových systémech,

Zranitelnost	Popis
	se kterými může aplikace komunikovat. V některých situacích může zranitelnost SSRF útočníkovi umožnit provedení libovolného spuštění příkazu. Zneužití SSRF, které umožní připojení k externím systémům třetích stran, může mít za následek škodlivé další útoky, které se zdají pocházet z organizace hostující zranitelnou aplikaci.

9.2 Seznam specifických zranitelností

Aktuálně bez specifických zranitelností testovaných specifickými testy.

Seznam testovacích scénářů: https://owasp.org/www-project-web-security-testing-guide/v42/

4.1 Information Gathering (Sběr informací)	
OTG-IG-001 - 4.1.1 **Conduct search engine discovery/reconnaissance for information leakage**	Zjistit, jaké citlivé informace o designu a konfiguraci aplikace, systému nebo organizace jsou vystaveny přímo na webových stránkách organizace (např. robots.txt) nebo nepřímo prostřednictvím služeb třetích stran (např. Shodan či Google)
OTG-IG-002 - 4.1.2 **Fingerprint Web Server**	Určit verzi a typ běžícího webového serveru, aby se zjistila známá zranitelná místa a příslušné zneužití, které je třeba použít při testování.
OTG-IG-003 - 4.1.3 **Review Webserver Metafiles for Information Leakage**	Identifikovat skryté nebo zmatené cesty a funkce pomocí analýzy metadat souborů. Analyzovat robots.txt použitím Google Webmaster Tools.
OTG-IG-004 - 4.1.4 **Enumerate Applications on Webserver**	Identifikovat aplikace, které existují v daném rozsahu. Black box pentest.
OTG-IG-005 - 4.1.5 **Review Webpage Comments and Metadata for Information Leakage**	Zkontrolovat komentáře a metadata webových stránek a najít možné úniky informací. Identifikovat soubory JavaScript a zkontrolovat jejich kód pro lepší porozumění aplikací a nalezení případného úniku informací. Zjistit zda existují soubory zdrojových map, a jaké jiné soubory vzniklé např. při ladění front-end.
OTG-IG-006 - 4.1.6 **Identify application entry points**	Analyzovat, jak jsou vytvářeny požadavky a typické odpovědi z aplikace.
OTG-IG-007 - 4.1.7 **Map executionpathsthroughapplication**	Mapování cílové aplikace a pochopení hlavních pracovních postupů.

OTG-IG-008 - 4.1.8 **Fingerprint Web Application Framework**	Definovat typ použitého webového rámce (např. WordPress, phpBB, Mediawiki atd.) pomocí známých otisků (http hlavičky, cookie, adresářové struktury) tak, aby se upřesnila metodika testování zabezpečení.
OTG-IG-009 - 4.1.9 **Fingerprint Web Application**	Identifikace webové aplikace a verze, aby se zjistili známá zranitelná místa a příslušné zneužití, které je třeba použít při testování.
OTG-IG-010 - 4.1.10 **Map Application Architecture**	Analyzovat architekturu aplikace a mapovat vzájemné vazby mezi aplikací a dalšími programy.
4.2 Configuration and Deployment Management Testing (Testování managementu konfigurace a nasazení)	
OTG-CONFIG-001 - 4.2.1 **Test Network/Infrastructure Configuration**	Otestovat konfiguraci infrastruktury, která podporuje aplikaci, identifikovat slabá místa v zabezpečení IS.
OTG-CONFIG-002 - 4.2.2 **Test Application Platform Configuration**	Přezkoumání a testování konfigurace. Testování přítomnosti defaultních nastavení, jako např. Directorytraversal vulnerability, Use ofsendmail.jsp atd.
OTG-CONFIG-003 - 4.2.3 **Test File Extensions Handling for Sensitive Information**	Určení způsobu, jakým webové servery zpracovávají požadavky odpovídající souborům s různými rozšířeními, mohou pomoci pochopit chování webového serveru v závislosti na druhu souborů, ke kterým je přístup.
OTG-CONFIG-004 - 4.2.4 **ReviewOld, Backup and Unreferenced Filesfor Sensitive Information**	Prověřit a vyhledat nereferenční nebo zapomenuté soubory, které lze použít k získání důležitých informací o infrastruktuře nebo pověřeních.
OTG-CONFIG-005 - 4.2.5 **Enumerate Infrastructure and Application Admin Interfaces**	Rozhraní správce mohou být nastaveny v aplikaci nebo na aplikačním serveru, což umožňuje určitým uživatelům provádět privilegované činnosti na webu. Provést testy s cílem zjistit, zda a jak může tato privilegovaná funkce získat přístup neoprávněnému nebo standardnímu uživateli.
OTG-CONFIG-006 - 4.2.6 **Test HTTP Methods**	Zjistit povolené http metody a možnosti jejich zneužití včetně CrossSiteTracing (XST).
OTG-CONFIG-007 - 4.2.7 **Test HTTP Strict Transport Security**	Ověřit, zda web používá hlavičku HTTP, aby bylo zajištěno, že všechna data budou šifrována z webového prohlížeče na server.
OTG-CONFIG-008 - 4.2.8 **Test RIA cross domain policy**	Rich Internet Application (RIA) používá politiku Adobe crossdomain.xml pro řízení crossdomain přístupů. Testovat konfiguraci soubory zásad popisujících omezení přístupu proti CSRF útokům.

OTG-CONFIG-009 - 4.2.9 **Test FilePermission**	Testovat konfiguraci oprávnění souboru pro ochranu před zneužitím eskalace privilegií, injekci DLL nebo neoprávněným přístupem k souborům.
OTG – CONFIG-010. - 4.2.10 **Test for Sudomain Takeover (nová)**	Detekovat všechny možné domény (předchozí i současné). Identifikovat zapomenuté nebo špatně nakonfigurované domény.
OTG – CONFIG-011 – 4.2.11 **Test Cloud Storage (nová)**	Ověřit nastavení konfigurace řízení přístupu pro služby úložiště.
4.3 Identity Management Testing (Testování managementu identit)	
OTG-IDENT-001 - 4.3.1 **Test Role Definitions**	Otestovat a pokusit se zachytit záhlaví paketů a jejich prohlížení. Využije se WebScarab nebo jiný libovolný webový proxy.
OTG-IDENT-002 - 4.3.2 **Test User Registration Process**	Ověřit, zda jsou požadavky na totožnost pro registraci uživatelů sladěny s požadavky definovaných politik a zabezpečení. Ověřit proces registrace, zda je validní.
OTG-IDENT-003 - 4.3.3 **Test Account Provisioning Process**	Prověřit existenci defaultních nebo snadno uhodnutelných uživatelských účtů. Ověřte, které účty mohou poskytovat další účty a jaký typ.
OTG- IDENT -004 - 4.3.4 **Testing for Account Enumeration and Guessable User Account**	Ověřit, zda je možné získat uživatelská jména interakcí s autentizačním mechanismem aplikace. Provést útok hrubou silou na přihlašovací údaje.
OTG- IDENT - 005 - 4.3.5 **Testing for Weak or unenforced username policy**	Prověřit, zda lze obejít autentizační mechanismus.
4.4 Autentification Testing (Testování Autentifikace)	
OTG-AUTH-001 - 4.4.1 **Testing for Credentials Transported over an Encrypted Channel**	Testovat, že uživatelská autentifikační data jsou přenášena přes šifrovaný kanál, aby se zabránilo zachycení útočníkem.
OTG- AUTH -002 - 4.4.2 **Testing for default credentials**	Provést test na přítomnost defaultních nebo známých uživatelských jmen a hesel pro zařízení v síti, která by vedla k úspěšné autentizaci.
OTG- AUTH -003 - 4.4.3 **Testing for Weak lock out mechanism**	Prověřit aplikaci na možnou zranitelnost mechanismu blokování účtů odolnost vůči brute-force útokům. Vyhodnotit odolnost mechanismu odblokování před neoprávněným odblokováním účtu.
OTG-AUTH-004 - 4.4.4 **Testing for Bypassing Authentication Schema**	Zjistit zda lze obejít autentifikační opatření tím, že manipulujete s žádostmi a podváděním aplikace, že si uživatel již ověřil. Toho lze dosáhnout buď úpravou daného parametru adresy URL, manipulací s formulářem nebo padělaním relací.

OTG- AUTH -005 - 4.4.5 **Testing for Vulnerable Remember Password**	Hledat hesla uložená v souboru cookie. Zkontrolovat soubory cookie uložené v aplikaci. Ověřit, zda pověření nejsou uložena v čistém textu, ale jsou šifrovaná. Prověřit mechanismus hashování: je-li to běžný, dobře známý algoritmus, zkontrolovat jeho sílu.
OTG- AUTH -005 - 4.4.6 **Testing for Browser cache weakness**	Testovat zranitelnost prohlížeče na dříve zadané citlivé informace.
OTG- AUTH -005 - 4.4.7 **Testing for Weak password policy**	Testovat odolnost aplikace před brute-force útokům uhádnutí hesla pomocí dostupných slovníků hesel vyhodnocením požadavků na délku, složitost, opětovné použití a exspiraci hesel.
OTG- AUTH -008 - 4.4.8 **Testing for Weak security question/answer**	Testovat na přítomnost lehce uhodnutelných otázek pro obnovu hesla.
OTG- AUTH -009 - 4.4.9 **Testing for weak password change or reset functionalities**	Určit odolnost aplikace proti možnosti změny účtu, která umožňuje někomu změnit heslo účtu. Určit odolnost funkce resetování hesel proti uhádnutí nebo obejití.
OTG- AUTH-010 - 4.4.10 **Testing for Weaker authentication in alternative channel**	Provedení testů k identifikaci alternativních kanálů a, v závislosti na rozsahu testování, identifikovat zranitelnosti autentifikace.
4.5 Authorization Testing (Prověření autorizace)	
OTG-AUTHZ-001 - 4.5.1 **Testing Directory traversal/file include**	Testovat odolnost aplikace vůči PathTraversal útoku.
OTG- AUTHZ -002 - 4.5.2 **Testing forby passing authorization schema**	Prověřit zda lze obejít autorizační mechanismus (např. přístup k funkcím/datům náležícím jiné uživatelské roli).
OTG- AUTHZ -003 - 4.5.3 **Testing for Privilege Escalation**	Prověřit aplikaci na zranitelnost typu eskalace privilegií.
OTG- AUTHZ -004 - 4.5.4 **Testing for Insecure Direct Object References**	Prověřit aplikaci na zranitelnost výskytu nesprávných odkazů na přímý objekt, když aplikace poskytuje přímý přístup k objektům založeným na uživatelském vstupu. V důsledku této zranitelnosti mohou útočníci obejít autorizaci a přístup k prostředkům přímo v systému, například databázové záznamy nebo soubory.
4.6 Session Management Testing (Správa relace)	
OWASP-SESS-001 - 4.6.1 **Testing for Session Management Schema**	Zkontrolovat cookie a jiné identifikátory relace zda jsou vytvořené bezpečným a nepředvídatelným způsobem.

OWASP- SESS -002 - 4.6.2 **Testing for Cookies attributes**	Prověřit správné nastavení cookie atributů.
OWASP- SESS -003 - 4.6.3 **Testing for Session Fixation**	Prověřit aplikaci na možnou zranitelnost session fixation (po úspěšné autentizaci se nezmění identifikátor relace).
OWASP- SESS -004 - 4.6.4 **Testing forExposed Session Variables**	Zjistit, zda jsou identifikátory relace dostatečně chráněné.
OWASP- SESS -005 - 4.6.5 **Testing for CSRF**	Testovat odolnost aplikace vůči CSRF útoku.
OWASP- SESS -006 - 4.6.6 **Testing for logout functionality**	Testovat možnost prvků uživatelského rozhraní, která umožňují uživateli ručně se odhlásit. Ověřit nastavení ukončení relace po určitém čase bez aktivity (časový limit relace). Ověřit správné zneplatnění stavu relace na straně serveru.
OWASP- SESS -007 - 4.6.7 **Test Session Timeout**	Otestovat že aplikace automaticky odhlásí uživatele, když byl uživatel po určitou dobu nečinný
OWASP- SESS -008 - 4.6.8 **Testing for Session puzzling**	Testovat zabezpečení aplikace na přítomnost a používání stejné proměnné relace pro více než jeden účel.
OWASP – SESS – 009 – 4.6.9 **Testing for Session Hijacking (nová)**	Identifikovat zranitelné soubory cookie. Unést zranitelné soubory cookie a posoudit úroveň rizika.
4.8 Input Validation Testing (Testování validace dat)	
OTG-INPVAL-001 - 4.7.1 **Testing for Reflected Cross Site Scripting**	Prověřit existenci nepersistentních XSS (Cross Site Scripting) zranitelností.
OTG- INPVAL -002 - 4.7.2 **Testing for Stored Cross Site Scripting**	Prověřit existenci persistentních XSS (Cross Site Scripting) zranitelností.
OTG- INPVAL -003 - 4.7.3 **Testing for http Verb Tampering (nová)**	Detekovat podporované metody HTTP. Otestovat možnosti obejití řízení přístupu. Otestovat chyby zabezpečení XST. Otestovat techniky přepsání metody HTTP.
OTG- INPVAL -004 - 4.7.4 **Testing for HTTP Parametr Pollution**	Prověřit existenci XSF (Cross Site Flashing) zranitelností.
OTG- INPVAL-005 - 4.7.5 **Testing for SQL Injection**	Prověřit existenci SQL Injection zranitelností.
OTG-DV-006 - 4.7.6 **Testing for LDAP Injection**	Prověřit existenci LDAP Injection zranitelností.
OTG-DV-007 – 4.7.7 **Testing for XML Injection**	Identifikovat body pro vložení XML. Posoudit typy exploitů, které lze využít, a jejich závažnost.

OTG-DV-008 – 4.7.8 **Testing for SSI Injection**	Prověřit existenci SSI Injection (Server-Side Includes) zranitelností.
OTG-DV-009 - 4.7.9 **Testing for XPath Injection**	Prověřit existenci XPath Injection (XML Path Language) zranitelností.
OTG-DV-010 - 4.7.10 **Testing for IMAP/SMTP Injection**	Prověřit existenci IMAP/SMTP zranitelností.
OTG-DV-011 - 4.7.11 **Testing for Code Injection**	Prověřit existenci Code Injection zranitelností.
OTG-DV-012 - 4.7.11.1 **Testing forLocal File Inclusion**	Prověřit existenci zranitelností (LFI) v podobě volání nějakého lokálního souboru skriptem.
OTG-DV-012 - 4.7.11.2 **Testing for Remote File Inclusion**	Prověřit existenci zranitelností (RFI) v podobě volání nějaké webové aplikace externím skriptem.
OTG-DV-012 - 4.7.12 **Testing for Command Injection**	Prověřit existenci zranitelností umožňující spuštění příkazů operačního systému.
OTG-DV-013 - 4.7.13 **Testing for Format String Injection (nová)**	Posoudit, zda vkládání specifikátorů převodu formátování řetězců do polí ovládaných uživatelem způsobí nežádoucí chování aplikace.
OTG-DV-014 - 4.7.14 **Testing for Incubated Vunerability**	Identifikovat injekce, které jsou uloženy a vyžadují krok znovu vyvolání. Pochopit/identifikovat, jak by mohlo ke znovu vyvolání dojít. Nastavit odposlech/záznam nebo, pokud je to možné, provést/zajistit znovu vyvolání injekce.
OTG-DV-015 - 4.7.15 **Testing for HTTP Splitting/Smuggling**	Prověřit existenci zranitelností v http hlavičce.
OTG-DV-016 - 4.7.16 **Testing for HTTP Incoming requests**	Prověřit existenci zranitelností v http vstupním požadavku.
OTG-DV-017 - 4.7.17 **Testing for Host HeaderInjection (nová)**	Posoudit, zda aplikace analyzuje hlavičky hostitele dynamicky. Obejít bezpečnostní prvky, které se spoléhají na hlavičky.
OTG-DV-018 – 4.7.18 **Testing for Server-Side Template Injection (nová)**	Zjistit body pro vložení vstupů do šablony. Identifikovat šablonovací modul. Připravit exploit.
OTG-DV-019-4.7.19 **Testing for Server-Side Request Forgery (nová)**	Identifikovat body pro SSRF injekci. Vyzkoušet, zda jsou tyto body zneužitelné. Ověřit závažnost zranitelnosti.
4.8 Testing for Error Handling (Testování zranitelností na dostupnost služeb)	
OTG-ERR-001 - 4.8.1 **Testing for Improper Error Handling**	Identifikovat existující chybový výstup. Analyzovat různé vrácené výstupy.

OTG-ERR-002 - 4.8.2 **Analysis of Stack Traces**	*Sloučeno s OTG-ERR-001 - 4.8.1*
4.9 Testing for weak Cryptography (Testování slabé kryptografie)	
OTG-CRYPST-001 - 4.9.1 **Testing for Weak Transport Layer Security**	Ověřit konfiguraci služby. Zkontrolovat sílu kryptografických algoritmů a platnost digitálního certifikátu. Ověřit, TLS není možné obejít a je správně implementováno v celé aplikaci.
OTG-CRYPST-002 - 4.9.2 **Testing for Padding Oracle**	Testovat na chyby „Padding Oracle“ neboli funkce aplikace, která dešifruje zašifrované údaje poskytované klientem, např. stavy interní relace uložené v klientovi a úniku stavu platnosti funkce po dešifrování. Existence této zranitelnosti umožňuje útočníkovi dešifrovat šifrované data a šifrovat libovolná data bez znalosti klíčů použitého pro tyto kryptografické operace.
OTG-CRYPST-003 - 4.9.3 **Testing for Sensitive information Sent via Unencrypted Channels**	Testovat na chyby zabezpečení přenosového kanálu, v kterém mohou být přenášeny informace v čistém textu. Zkontrolovat, zda jsou tyto informace přenášeny přes protokol HTTP namísto protokolu HTTPS nebo zda jsou používány slabé Cypher algoritmy.
OTG-CRYPST-004 - 4.9.4 **Testing for Weak Encryption**	Testovat na přítomnost slabých kryptokódů.
4.10 Business logic testing (Prověření logiky aplikace)	
OTG-BUSLOGIC-001 - 4.10.1 **Testing for Business Logic data validation**	Testovat na chyby v logice aplikace umožňující uživateli provést operaci s daty jiným způsobem než bylo navrženo.
OTG-BUSLOGIC-002 - 4.10.2 **Test Ability to Forge Requests**	Testovat zranitelnosti vůči využití proxy k odeslání žádostí HTTP POST / GET do aplikace Zkontrolujte projektovou dokumentaci a použijte průzkumné testování, které hledá odhadnutelnou, předvídatelnou nebo skrytou funkcionalitu polí.
OTG-BUSLOGIC-003 - 4.10.3 **Test integrity checks**	Testovat na chyby v zajištění integrity aplikace. Odolnost vůči nepovolenému odeslání hodnot skrytých polí serveru pomocí serveru proxy.
OTG-BUSLOGIC-004 - 4.10.4 **Test for Process Timing**	Testovat na časové odezvy při nesprávném zadání autentifikačních údajů.
OTG-BUSLOGIC-005 - 4.10.5 **Test Number of Times a Function Can Be Used Limits**	Zkontrolovat projektovou dokumentaci a použiít testování, které hledá funkce nebo funkce v aplikaci nebo systému, které by neměly být prováděny více než jednou nebo pouze určitým počtem opakování během pracovního postupu v aplikaci.

OTG-BUSLOGIC-006 - 4.10.6 **Testing for the Circumvention of Work Flows**	Testovat na chyby v logice aplikace umožňující uživateli provést operaci s daty jiným způsobem než bylo navrženo.
OTG-BUSLOGIC-007 - 4.10.7 **Test Defenses Against Application Misuse**	Testovat na přítomnost obranných mechanismů v aplikační vrstvě, které chrání aplikaci proti nesprávnému použití nebo neplatnému použití platné funkce, které se snaží kompromitovat webovou aplikaci, identifikovat slabé stránky a zneužívat zranitelnosti.
OTG-BUSLOGIC-008 - 4.10.8 **Test Upload of Unexpected File Types**	Testovat mechanismus ověřování správného typu souborů. Aplikace může očekávat, že budou na zpracovávány pouze určité typy souborů, jako jsou soubory .CSV, .txt. Aplikace musí ověřovat nahraný soubor buď podle přípony (pro ověření souboru s nízkou jistotou) nebo podle obsahu (ověření souboru s vysokou jistotou). To může vést k neočekávaným výsledkům systému nebo databáze v rámci aplikace / systému nebo k tomu, že útočníkům poskytnou další metody pro využití aplikace / systému.
OTG-BUSLOGIC-009 - 4.10.9 **Test Upload of Malicious Files**	Testovat na zranitelnost vůči škodlivým kódům.
4.11 ClientSide Testing (Testování klienta)	
OTG-CLIENT-001 - 4.11.1 **Testing for DOM-based Cross Site Scripting**	Prověřit existenci DOM (document object model) XSS zranitelností.
OTG-CLIENT-002 - 4.11.2 **Testing for JavaScript Execution**	Otestovat provádění JAVA skriptů a ověřit, zda nelze získat osobní data uživatele nebo upravit obsah web stránky, kterou uživatel může vidět. Chyba zabezpečení typu JavaScript Injection je podtyp Cross Scriptingu (XSS), který zahrnuje možnost vkládat libovolný kód JavaScript, který aplikace provádí uvnitř prohlížeče oběti.
OTG-CLIENT-003 - 4.11.3 **Testing for HTML Injection**	Prověřit odolnost vůči zranitelnosti typu HTML injection.
OTG-CLIENT-004 - 4.11.4 **Testing forClientSide URL Redirect**	Zkontrolovat odolnost aplikace, když aplikace přijímá nedůvěryhodný vstup, který obsahuje hodnotu URL, aniž by jej dezinfikoval. Odolnost vůči přesměrování webové aplikace na jinou stránku.
OTG-CLIENT-005 - 4.11.5 **Testing for CSS Injection**	Prověřit odolnost vůči zranitelnosti typu CSS Injection.
OTG-CLIENT-006 - 4.11.6 **Testing for Client Side Resource Manipulation**	Otestovat odolnost vůči zranitelnosti typu Client Side Resource Manipulation.

OTG-CLIENT-007 - 4.11.7 **Test Cross Origin Resource Sharing**	Prověřit používání CORS a otestovat, že není změněn Java scriptem. Otestovat protokoly na úrovni aplikace, že se používají k ochraně citlivých dat.
OTG-CLIENT-008 - 4.11.8 **Testing for Cross Site Flashing**	Prověřit existenci XSF (Cross Site Flashing) zranitelností.
OTG-CLIENT-009 - 4.11.9 **Testing for Click jacking**	Otestovat odolnost vůči útokům typu Click jacking
OTG-CLIENT-010 - 4.11.10 **Testing Web Sockets**	Prověřit zda je webová služba přístupná přes HTTP a zda server ověřuje hlavičku Origin v počátečním handshake HTTP WebSocket. Pokud server neověřuje záhlaví původu v počátečním handshake serveru Web Socket, server Web Socket může přijímat připojení z libovolného původu.
OTG-CLIENT-011 - 4.11.11 **Testing Web Messaging**	Je třeba provést ruční testování a kód JavaScript analyzovat hledáním implementace služby Web Messaging. Zejména je třeba prověřit, jak webové stránky omezují zprávy z nedůvěryhodné domény a jak se s nimi zachází i pro důvěryhodné domény
OTG-CLIENT-012 – 4.11.12 **Testing Brower Storage**	Zjistit, zda web ukládá citlivá data do úložiště na straně klienta. Prozkoumat zpracování kódu objektů úložiště z hlediska možností injekčních útoků, jako je využití nevalidovaného vstupu nebo zranitelných knihoven.
OTG-CLIENT-013– 4.11.13 **Testing for Cross Site Script Inclusion (nová)**	Vyhledat citlivá data v celém systému. Pomocí různých technik vyhodnotit možnost úniku citlivých dat.
4.12 API Testing (nová)	
OTG-API – 01-4.12.1 **Testing Graph QL (nová)**	Ověřit, že je nasazena bezpečná a připravená konfigurace. Ověřit všechna vstupní pole proti obecným útokům. Zajistit, aby byly použity správné metody řízení přístupu.

Příloha č. 07 – Pravidla pro dodavatele - minimální bezpečnostní standard pro významné dodavatele

Český úřad zeměměřický a katastrální přijal minimální bezpečnostní standard pro dodavatele dle požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále jen „ZoKB“) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „VoKB“).

1. Obecné požadavky na Dodavatele

1.1. Dodavatel se zavazuje dodržovat obecně závazné právní předpisy.

1.2. Dodavatel se zavazuje, že má pro plnění předmětu smlouvy plně nastavené a využívané procesy k zajištění bezpečnosti informací v souladu s ISO/EC 27001.

1.3. Pro realizaci předmětu plnění má Dodavatel právo použít smluvní Poddodavatele. Seznam Poddodavatelů předložil Dodavatel před podpisem smlouvy. Dodavatel má právo použít k plnění i další Poddodavatele po předchozím odsouhlasení Objednatelem. Objednatel odsouhlasení nového Poddodavatele bezdůvodně neodmítne. V případě, že Dodavatel využívá Poddodavatele k výkonu činností vymezených ve smlouvě, odpovídá za kvalitu, bezpečnost a včasnost plnění stejným způsobem, jako by činnost prováděl sám.

1.4. V případě, že Dodavatel využívá Poddodavatele k výkonu činností definovaných smlouvou, je povinen informovat Poddodavatele o požadavcích na bezpečnost informací a bezpečnostních pravidlech, které je povinen dodržovat při výkonu dané činnosti alespoň ve stejném rozsahu, v jakém od Dodavatele Objednatel požaduje. Dodavatel je povinen Objednatele předem informovat o významné změně ovládání Dodavatele. Ovládáním se zde rozumí zejména ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení. Notifikační povinnost může být taktéž navázána na změnu skutečného majitele v evidenci skutečných majitelů (§ 118b a násl. zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřeneckých fondů).

1.5. Objednatel je oprávněn bez jakýchkoliv sankcí odstoupit od smlouvy v případě významné změny kontroly Dodavatele s tím, že změnou kontroly Dodavatele se rozumí změna ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, změna vlastnictví zásadních aktiv, popřípadě změna oprávnění nakládat s těmito aktivy, využívanými Dodavatelem k plnění Smlouvy.

1.6. Dodavatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 5 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Dodavatel se zavazuje řídit rizika spojená s plněním Smlouvy. Dodavatel je povinen neprodleně informovat Objednatele o výsledcích analýzy rizik a možných rizicích spojených s poskytováním služeb Objednateli, výsledcích analýzy rizik a přijatých opatřeních. Dodavatel nesmí přijmout rizika spojená s poskytováním služeb Objednateli bez písemného souhlasu Objednatele.

1.7. Objednatel si vyhrazuje právo provádět u Dodavatele zákaznické audity zaměřené na plnění procesních, bezpečnostních a legislativních povinností při poskytování služeb Objednateli nebo zpracování údajů Objednatele. Dodavatel bere na vědomí, že po dobu trvání smlouvy umožní Objednateli zejména provést kontrolu souladu s požadavky ZoKB a souvisejících právních předpisů.

1.8. Dodavatel se zavazuje neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech (viz § 7 ZoKB) a poskytovat nezbytnou součinnost při plnění požadavků specifikovaných v § 8 ZoKB. Dodavatel se dále zavazuje

poskytnout nezbytnou součinnost potřebnou pro vyšetření a případné vyřešení daného kybernetického bezpečnostního incidentu.

1.9. Dodavatel se zavazuje určit osobu odpovědnou ze smlouvy za plnění bezpečnostních požadavků, do 14 dnů od doručení tohoto bezpečnostního standardu, pokud tato osoba není již smlouvou definovaná.

1.10. Dodavatel je povinen vést písemnou evidenci aktiv, které využívá k plnění smlouvy (aktivem jsou např. data, informace, SW, HW, lidské zdroje, prostory, licence, Poddodavatele), tuto evidenci zpřístupní na vyžádání Objednatele.

1.11. Dodavatel se zavazuje pro případ, že se v průběhu plnění předmětu Smlouvy dostane do kontaktu s osobními údaji, že je bude ochraňovat a nakládat s nimi plně v souladu s příslušnými právními předpisy, tj. zejména se zákonem č. 110/2019 Sb., o zpracování osobních údajů, a Obecným nařízením o ochraně osobních údajů (GDPR - Nařízení Evropského parlamentu a Rady (EU) 2016/679), tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich zneužití, změně, zničení či ztrátě, a to i po ukončení plnění smlouvy. Dodavatel se zavazuje pro případ, že se v průběhu plnění předmětu smlouvy dostane do kontaktu s údaji Objednatele vyplývajícími z jeho provozní činnosti, tyto údaje v žádném případě nezneužít, nezveřejnit, nepředat třetí osobě, nezměnit, ani jinak nepoškodit, ztratit či znehodnotit.

1.12. Dodavatel se zavazuje nejpozději do 15 dnů od doručení tohoto oznámení prokazatelně seznámit všechny osoby podílející se na plnění předmětu smlouvy s bezpečnostními požadavky. O seznámení jsou vedeny písemné záznamy.

1.13. Smluvní strany se v případě, že se Dodavatel dostane do pozice zpracovatele osobních údajů ve správě Objednatele, ve smyslu příslušných ustanovení zákona o ochraně osobních údajů, zavazují uzavřít dodatek ke smlouvě spočívající v dohodě o zpracování osobních údajů, pokud platná smlouva toto již nezahrnuje.

2. Ochrana osobních údajů

2.1. Dodavatel je povinen zajistit, aby do informačních systémů Objednatele obsahující informace s osobními údaji měli přístup pouze zaměstnanci, kteří k tomu mají oprávnění.

2.2. Objednatel je povinen každému zaměstnanci, který má přístup do informačních systémů s informacemi a osobními údaji Dodavatele, vydat osobní a jedinečný identifikační kód pro tyto účely - uživatelské ID. Uživatelské ID nesmí být nikdy ani v budoucnu postoupeno jiné osobě.

2.3. Dodavatel je povinen zajistit, aby jeho zaměstnancům nebo zaměstnancům Poddodavatele bylo povoleno zpracovávat informace a Osobní údaje Objednatele, pouze pokud jim jsou přiděleny ověřovací údaje (credentials), např. k úspěšnému provedení ověřovacího postupu týkajícího se buď specifické operace zpracování, nebo sady operací zpracování.

2.4. Objednatel je povinen deaktivovat ověřovací údaje, pokud je zaměstnanec Dodavatele prohlášen nezpůsobilým nebo mu je odebráno oprávnění přístupu do informačních systémů Objednatele nebo ke zpracování informací a osobních údajů Objednatele.

2.5. Zaměstnanci Dodavatele mohou mít oprávněný přístup pouze k těm údajům a zdrojům, které jsou nezbytné pro plnění jejich povinností – tzv. princip need-to-know.

2.6. Dodavatel je povinen zajistit, aby informační systémy Objednatele a hmotné nosiče, na kterých jsou uloženy informace a Osobní údaje Objednatele, byly u Dodavatele uschovány v bezpečném prostředí znemožňující vyzrazení, modifikaci, zničení či jiné ovlivnění informací a osobních údajů Objednatele.

2.7. Dodavatel je povinen zajistit, aby nosiče obsahující informace a Osobní údaje Objednavatele byly u Dodavatele k dispozici pouze pověřeným zaměstnancům.
2.8. Dodavatel je povinen zajistit, aby informace a Osobní údaje Objednatele byly od Dodavatele distribuovány prostřednictvím veřejných elektronických komunikačních sítí pouze tehdy, pokud jsou zakódovány nebo jinak zašifrovány nebo je použit jiný mechanismus zajišťující, aby údaje nebyly srozumitelné nebo aby s nimi nemohly manipulovat třetí osoby.
2.9. Dodavatel je povinen zaznamenávat přístup všech zaměstnanců Dodavatele/Poddodavatele do informačních systémů Objednatele, ve kterých jsou zpracovány informace nebo Osobní údaje Objednatele, a to tak, aby přístup byl bezpečně dohledatelný a identifikovatelný.
2.10. Minimální doba pro uchování zaznamenaných údajů je 18 měsíců.
2.11. Dodavatel je povinen zajistit, aby přístup do prostor u Dodavatele, kde jsou umístěny informační systémy a nosiče Objednatele s uloženými informacemi a Osobními údaji Objednatele, měli pouze zaměstnanci, kteří mají přidělena řádná oprávnění a kteří mají oprávněný důvod ke vstupu.
2.12. Dodavatel je povinen zajistit postup nahlašování bezpečnostních incidentů, reagování na ně a jejich vyřizování.
2.13. Dodavatel je povinen v rámci procesu pro šetření bezpečnostních incidentů zajistit, že Objednatel bude bezodkladně informován o jakémkoli bezpečnostním incidentu, který má či může mít vliv na informace a Osobní údaje Objednatele.
2.14. Dodavatel je povinen přijmout nezbytná opatření, aby zaměstnanci byli dobře obeznámeni s těmito minimálními bezpečnostními požadavky a s následky jakéhokoliv jejich porušení.
2.15. Dodavatel je povinen zajistit, aby jeho zaměstnanci byli vázáni povinností mlčenlivosti o informacích, Osobních údajích Objednatele a bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení informací a osobních údajů Objednatele, přičemž tato povinnost trvá i po skončení zaměstnání nebo příslušných prací.
2.16. Dodavatel je povinen zajistit, aby při ukončení smlouvy byly informace a Osobní údaje Objednatele předány a následně smazány z nosičů, informačních systémů a dalších zařízení Dodavatele (včetně bezpečnostních záloh). O smazání dokumentů bude předáno Objednavateli čestné prohlášení.
2.17. Zaměstnanci Dodavatele jsou povinni zejména:
    2.17.1. odpovídajícím způsobem chránit informace a Osobní údaje Objednatele, a to zcela bez ohledu na jejich formu uložení (flash disky, mobilní telefony, papírové dokumenty, notebooky, disky, vyměnitelná média apod.),
    2.17.2. obrátit se na Objednatele s žádostí o pomoc, pokud by hrozilo, že jakýmkoli způsobem bude ohroženo plnění povinností dle tohoto Minimálního bezpečnostního standardu.
2.18. Zaměstnanci Dodavatele se musí zdržet zejména:
    2.18.1. předávání Osobních údajů a dalších chráněných informací Objednatele jakýmkoli neoprávněným osobám,
    2.18.2. předávání Osobních údajů Objednatele prostřednictvím veřejně dostupných cloudových služeb (jako je např. Dropbox, Google disk apod.).
2.19. Dodavatel nemá oprávnění k využití dat pro svou potřebu, např. statistické účely, evidenční podklady vyúčtování apod.

3. Organizační bezpečnost

3.1. Dodavatel se zavazuje vést provozní deník, kde budou zaznamenány všechny podstatné okolnosti vzniklé s plněním smlouvy.
3.2. Dodavatel se zavazuje řídit přístupy a oprávnění zaměstnanců tak, aby minimalizoval neoprávněný přístup k aktivům Objednatele.
3.3. Dodavatel je povinen dodržovat platné smluvní podmínky výrobců a dodržovat licenční čistotu dle zákona o autorském právu č. 121/2000 Sb.
3.4. Dodavatel je povinen vést systémovou a provozně technickou bezpečnostní dokumentaci.

4. Řízení kontinuity činností a obnovy po havárii

4.1. Dodavatel je povinen ve spolupráci s Objednatelem pracovat na přípravě plánů obnovy po havárii, případně poskytnout nezbytnou součinnost pro jejich přípravu.
4.2. Všechny připravené plány obnovy po havárii budou Objednatelem v pravidelných intervalech testovány na svou účinnost a proveditelnost. Dodavatel je povinen se daného testování v nezbytné míře zúčastnit. O termínu testování bude Dodavatel v dostatečném předstihu informován Objednatelem.
4.3. V případě zjištění nedostatků v testovaných plánech obnovy po havárii je Dodavatel povinen v patřičném rozsahu dané plány upravit dle výsledků testování tak, aby byly proveditelné a účinné.
4.4. V případě výskytu havárie Dodavatelem dodávaného systému je Dodavatel povinen účastnit se jeho obnovy v rozsahu stanoveném připravenými plány obnovy po havárii.

5. Audit kybernetické bezpečnosti

5.1. Dodavatel bere na vědomí, že po celou dobu smlouvy je povinen poskytnout Objednateli nezbytnou součinnost pro ověření, zda Dodavatel splňuje požadavky ZoKB.
5.2. Objednatel je povinen písemně sdělit Dodavateli termín, místo a nezbytný rozsah auditu nejpozději 14 dní před zahájením auditu.
5.3. Objednatel je povinen písemně sdělit jména osob, která se budou auditu účastnit. Tyto osoby mohou zahrnovat i osoby třetích stran.
5.4. Objednatel je povinen informovat o výsledcích auditu Dodavatele nejpozději do 30 dnů od jeho skončení.
5.5. Dodavatel je povinen poskytnout nezbytnou součinnost, předložit na vyžádání dokumenty a realizovat schválená nápravná opatření.

6. Technická opatření

Dodavatel se zavazuje po dobu trvání smlouvy realizovat technická opatření a dodržovat požadavky:

6.1. Požadavky na zajištění fyzické bezpečnosti dle § 17 VoKB k zajištění ochrany aktiv a zamezení neoprávněného vstupu, a to především
  6.1.1. definovat bezpečnostní zóny k zabezpečení v minimálním rozsahu (serverovna, uživatelské prostory, prostory dostupné pro třetí strany),
  6.1.2. definovat pro jednotlivé bezpečnostní zóny vhodná bezpečnostní opatření na zajištění proti neoprávněnému vstupu, přičemž zóna typu serverovna

musí mít automaticky řízený a evidovaný systém vstupů, musí být zajištěna proti vniknutí, a musí být chráněna před požárem a vysokou teplotou,

6.1.3. zajistit, aby všechny zóny byly náležitě monitorovány pro případnou detekci neoprávněného vstupu a předcházení poškození umístěného vybavení.

6.2. Požadavky na zajištění bezpečnosti komunikačních sítí dle § 18 VoKB, tj, segmentace sítě, zajištění důvěrnosti a integrity vzdáleného připojení, využití nástroje k zajištění integrity sítě, a to především

6.2.1. síť musí být rozdělena do několika logických síťových segmentů dle funkce či účelu (typicky uživatelský segment, IT segment, serverový segment, tiskový segment, DMZ apod.),

6.2.2. komunikace mezi jednotlivými segmenty musí být automaticky řízena a kontrolována na úrovni firewallu definujícího komunikační pravidla mezi segmenty,

6.2.3. v rámci sítě musí být aktivně blokovány potenciálně nebezpečné komunikační protokoly, typicky Telnet, FTP, SNMPv1/SNMPv2, POP3, IMAP apod.,

6.2.4. přístup k interní síti musí být kontrolován a povolen jen oprávněným uživatelům/zařízením, např. pomocí 802.1x,

6.2.5. při používání vzdáleného přístupu musí být takové vzdálené spojení šifrované za použití protokolů doporučených Národním úřadem pro kybernetickou a informační bezpečnost.

6.3. Požadavky správy a ověřování identit dle § 19 VoKB, a to především

6.3.1. identity všech uživatelů, administrátorů a aplikací musí být spravovány centrálním nástrojem, např. Active Directory, IdM apod.,

6.3.2. před přihlášením uživatele musí dojít k ověření jeho identity,

6.3.3. po pěti neúspěšných pokusech o přihlášení uživatele musí dojít k zablokování jeho účtu alespoň na dobu 30 minut,

6.3.4. přihlašovací údaje musí být uloženy v šifrované formě a odolné proti odcizení, zneužití a případným útokům,

6.3.5. při nečinnosti uživatele po dobu delší než 15 minut musí dojít k odhlášení uživatele či uzamčení jeho sezení a uživatel musí být donucen znovu poskytnout své přihlašovací údaje,

6.3.6. pro přihlašování uživatelů musí být použita vícefaktorová autentizace,

6.3.7. není-li možné využít vícefaktorovou autentizaci, musí být používána autentizace pomocí kryptografických klíčů,

6.3.8. není-li možné využít autentizace pomocí kryptografických klíčů, musí být vynucena politika hesel

6.3.8.1. hesla uživatelů musejí mít minimální délku 12 znaků,

6.3.8.2. hesla administrátorů a technických či servisních účtů musejí mít minimální délku 17 znaků,

6.3.8.3. uživatelé musejí mít možnost použít hesla alespoň 64 znaků dlouhá,

6.3.8.4. heslo musí obsahovat alespoň jedno malé a jedno velké písmeno, číslici a speciální znak,

6.3.8.5. uživatelé si mohou změnit heslo nejdříve 24 hodin od poslední změny hesla,

6.3.8.6. nesmějí být používána nejčastěji používaná hesla, např. „heslo“, „123456“, „qwertz“ apod.

6.3.8.7. heslo nesmí obsahovat mnohokrát se opakující znaky, přihlašovací jméno, e-mail, název systému apod.,

6.3.8.8. uživatelé při změně hesla nesmějí použít žádné z předchozích 12 hesel,

6.3.8.9. po maximálně 18 měsících musí docházet k vynucené změně hesla,
6.3.8.10. při vytvoření úvodního hesla nebo hesla pro obnovení musí být toto heslo po jeho prvním použití ihned zneplatněno a uživatel musí být nucen zvolit si své vlastní,
6.3.8.11. uživatelé musejí být informování o politice hesel.

6.4. Požadavky na řízení přístupových oprávnění dle § 20 VoKB, a to především
6.4.1. pro přidělování uživatelských oprávnění je zaveden centrální systém,
6.4.2. oprávnění jsou přidělována na základě evidované žádosti, která je schválena oprávněnou osobou,
6.4.3. všechna přidělená oprávnění jsou pravidelně revidována (alespoň jednou ročně) a nepotřebná oprávnění jsou odebírána.

6.5. Požadavky na ochranu před škodlivým kódem dle § 21 VoKB, a to především
6.5.1. dodavatel bude využívat nástroj na ochranu před škodlivým kódem instalovaný alespoň na koncových stanicích, serverech, datových úložištích, prvcích komunikační sítě a přiměřeně na mobilních zařízeních,
6.5.2. virové definice daného nástroje musejí být aktualizovány alespoň jednou za den,
6.5.3. při vydání nové verze nástroje musí být instalována aktualizace nejpozději do 3 měsíců od publikace,
6.5.4. musí být aktivně řízeno používání vyměnitelných médií – jejich použití musí být omezeno jen na vybrané pracovníky, kteří je nutně potřebují pro výkon své práce,
6.5.5. při používání vyměnitelných zařízení musí být jejich obsah oskenován nástrojem na ochranu před škodlivým kódem předtím, než k němu může přistoupit uživatel,
6.5.6. uživatelé nesmějí mít možnost spustit neautorizovaný software.

6.6. Požadavky na zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů v rozsahu § 22 VoKB, a to především
6.6.1. provozní a bezpečnostní události na aktivech souvisejících s poskytováním služby jsou zaznamenávány alespoň v rozsahu § 22 odst. 2 písm. d) VoKB,
6.6.2. zaznamenané události musí obsahovat alespoň informace uvedené v § 22 odst. 2 písm. b) VoKB,
6.6.3. zaznamenané události jsou uchovávány v centrálním úložišti po dobu alespoň 18 měsíců, kde musí být zajištěna jejich integrita,
6.6.4. napříč prostředím Dodavatele musí docházet k synchronizaci času s jednotným zdrojem času,
6.6.5. v případě kybernetických bezpečnostních událostí/incidentů bude možné předat příslušné logy Objednateli.

6.7. Požadavky na detekce kybernetických událostí dle § 23 VoKB, a to především:
6.7.1. v prostředí sítě dojde k implementaci nástroje IPS umožňujícího identifikaci a případnou blokaci nežádoucí komunikace jak v rámci interní sítě, tak mezi dalšími sítěmi, např. internetem,
6.7.2. záznamy o takové komunikaci budou ukládány do centrálního úložiště logů.

6.8. Požadavky na sběr a vyhodnocování událostí dle § 24 VoKB, a to především
6.8.1. v rozsahu služeb poskytovaných Objednatel nasadí Dodavatel nástroj typu SIEM pro vyhodnocování kybernetických bezpečnostních událostí,
6.8.2. vyhodnocování bude probíhat nad logy, které jsou ukládány v rámci centrálního úložiště,
6.8.3. informace o potenciálních kybernetických bezpečnostních incidentech bude předávána osobě s kompetencí kybernetické bezpečnosti k vyhodnocení,

6.8.4. informace z nástroje budou používány pro průběžné zlepšování zabezpečení prostředí Dodavatele v rozsahu poskytovaných služeb.

6.9. Požadavky na aplikační bezpečnost dle § 25 VoKB, a to především

6.9.1. poskytuje-li dodavatel Objednateli aplikaci či jiný informační systém, zajistí před jeho nasazením do provozu v prostředí Objednatele penetrační test a zajistí nápravu všech zjištěných zranitelností ohodnocených skórem CVSS v3 7.0 a vyšší, případně všechny vysoké a kritické zranitelnosti, není-li používáno skóre CVSS,

6.9.2. obdobně postupuje Dodavatele v případě, kdy připravuje významnou změnu daného systému.

6.10. Požadavky na kryptografické prostředky dle § 26 VoKB, a to především

6.10.1. využívá-li Dodavatel při poskytování služby Objednateli kryptografických prostředků, musí být používány pouze takové kryptografické algoritmy, které doporučuje Národní úřad pro kybernetickou a informační bezpečnost,

6.10.2. využívá-li k tomuto účelu Dodavatel vlastních klíčů a certifikátů, zajistí zabezpečení životního cyklu těchto kryptografických prostředků.

6.11. Požadavky na zajištění úrovně dostupnosti informací dle § 27 VoKB, a to především v případě, kdy poskytuje Dodavatel informační systém jako službu, případně přímo zajišťuje jeho provoz a další rozvoj, zajistí ve spolupráci s Objednatelem jeho dostupnost dle výsledků provedené analýzy dopadů na straně Objednatele.

6.12. Požadavky na bezpečnost průmyslových, řídících a obdobných systémů dle § 28 VoKB, a to především poskytuje-li Dodavatel Objednateli systémy spadající do kategorie průmyslové, řídicí a obdobné systémy, zajistí jejich kybernetickou bezpečnost specifickými opatřeními

6.12.1. systém bude provozován v komunikační síti oddělené od ostatní infrastruktury,

6.12.2. vzdálený přístup k takovému systému bude omezen pouze na specifické IP adresy po vyhrazené komunikační lince oddělené od běžného vzdáleného přístupu,

6.12.3. na úrovni komunikační sítě musí být aktivně blokována komunikace vedoucí na potenciálně zranitelná rozhraní daného systému,

6.12.4. v případě výpadku systému musí existovat detailní postup pro obnovu jeho chodu.

6.13. Dodavatel se zavazuje plnit požadavky na likvidaci médií dle přílohy 4 VoKB.