**Smlouva na dodávku GIS SW systému pro data INSPIRE,**

**licencí SW a souvisejících služeb**

Číslo 2022/065 NAKIT

Smluvní strany

##### Národní agentura pro komunikační a informační technologie, s. p.

se sídlem Kodaňská 1441/46, Vršovice, 101 00 Praha 10

IČO: 04767543

DIČ: CZ04767543

zastoupen: xxx

zapsán v obchodním rejstříku vedeném Městským soudem v Praze oddíl A vložka 77322 bankovní spojení xxx

č.ú. xxx

(dále jen „**Objednatel**“) a

##### Společnost SEVITECH

vzniklá na základě smlouvy o společnosti uzavřené dne 26. 1. 2022 mezi níže uvedenými společně a nerozdílně zavázanými společníky:

SEVITECH CZ s.r.o.

se sídlem Na strži 2102/61a, Krč, 140 00 Praha 4

IČO: 07081561

DIČ: CZ07081561

zastoupen: xxx

zapsán v obchodním rejstříku vedeném Městským soudem v Praze oddíl C vložka 294361 bankovní spojení xxx

č.ú. xxx

(dále jen „**Vedoucí společník**“)

SYNCHRONIX a.s.

se sídlem Mlynské nivy 71, Bratislava 821 05

IČO: 31 605 052

DIČ: 2020444338

zastoupen: xxx a xxx

zapsán v obchodním rejstříku vedeném Okresním soudem Bratislava I. oddíl: Sa, vložka 4696/B

(dále jen „**Druhý společník**“)

Ve vztahu k Objednateli a této Smlouvě je za Společnost SEVITECH oprávněn jednat její Vedoucí společník, tj. SEVITECH CZ s.r.o.

(dále Společnost SEVITECH jen jako „**Dodavatel**“)

dále jednotlivě jako „**Smluvní strana**“, nebo společně jako „**Smluvní strany**“ uzavírají v souladu s ustanovením § 1746 odst. 2 a § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“) a zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**AZ**“) tuto Smlouvu na dodávku GIS SW systému pro data INSPIRE, licencí SW a souvisejících služeb (dále jen „**Smlouva**“).

##### Preambule

Objednatel provedl v souladu s ustanoveními zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), zadávací řízení k veřejné zakázce

##### „Dodání komponent a rolí pro zajištění dalších činností v rámci projektu ISSI II.“ (dále jen

„**Zadávací řízení**“) na uzavření této Smlouvy. Smlouva je uzavřena s Dodavatelem na základě výsledku Zadávacího řízení. Objednatel tímto ve smyslu ust. § 1740 odst. 3 občanského zákoníku předem vylučuje přijetí nabídky na uzavření této Smlouvy s dodatkem nebo odchylkou.

V souvislosti s touto Smlouvou byly uzavřeny mezi tentýž Smluvními stranami ještě Rámcová dohoda na poskytování integračních a konfiguračních služeb a Smlouva o poskytnutí Podpory GIS Systému, kdy tyto tři smlouvy tvoří společně předmět shora uvedené veřejné zakázky a jsou uzavírány se společným účelem. Tyto tři shora uvedené smlouvy na sebe vzájemně navazují a je nezbytné je vykládat ve vzájemné souvislosti.

##### Úvodní ustanovení a účel Smlouvy

* 1. Účelem této Smlouvy je zajištění kompletního zpracování definovaných dat v rámci INSPIRE (Infrastruktura pro prostorová data v Evropě) a dodávka, zajištění provozu a

rozvoje Geografického informačního systému pro data INSPIRE (dále jen „**GIS Systém**“ jak je tento pojem definován v čl. 2 odst. 2.1 písm. a) této Smlouvy) v rámci ISSI (Informační systém pro veřejné služby a služby veřejné správy INSPIRE), to vše v souladu s požadavky Objednatele definovanými touto Smlouvou a za účelem plnění závazků Objednatele vůči Ministerstvu vnitra České republiky, (dále jen „**Koncový zákazník**“ nebo „**MV**“), a to tak, aby Objednatel mohl systém začlenit do většího celku, užívat, poskytovat k užívání MV, udržovat a rozvíjet, a to samostatně nebo prostřednictvím třetí osoby.

* 1. Dodavatel prohlašuje, že:
		1. je oprávněn uzavřít Smlouvu a plnit své povinnosti vyplývající ze Smlouvy;
		2. na straně Dodavatele není k uzavření Smlouvy ani ke splnění závazků Dodavatele z ní vyplývajících požadován žádný souhlas, udělení výjimky, schválení, prohlášení ani povolení jakékoliv třetí osoby či orgánu, popřípadě byly získány;
		3. uzavření Smlouvy Dodavatelem není (i) porušením jakékoliv povinnosti vyplývající z platných právních předpisů v jakémkoliv právním řádu, jímž je Dodavatel vázán, a/nebo (ii) porušením jakékoliv povinnosti vyplývající z jakékoliv smlouvy, jíž je Dodavatel stranou, a/nebo (iii) v rozporu s jakýmkoliv požadavkem, rozhodnutím nebo předběžným opatřením správního orgánu nebo soudu nebo rozhodčím nálezem rozhodců, jímž je Dodavatel vázán;
		4. splňuje veškeré požadavky na jeho způsobilost (kvalifikaci) stanovené

v Zadávacím řízení;

* + 1. Dodavatel není v úpadku nebo v hrozícím úpadku ve smyslu § 3 zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), v platném znění. Proti Dodavateli nebyl podán (i) insolvenční návrh, nebo (ii) návrh na nařízení výkonu rozhodnutí, resp. obdobný návrh v příslušné jurisdikci či podle dříve platných českých právních předpisů, a podle nejlepšího vědomí Dodavatele podání takového návrhu ani nehrozí;
		2. nebyl předložen žádný návrh, ani učiněno žádné rozhodnutí příslušných orgánů Dodavatele ani žádného soudu o likvidaci Dodavatele nebo o jakékoliv jeho přeměně ve smyslu zákona č. 125/2008 Sb., o přeměnách obchodních společností a družstev, ve znění pozdějších předpisů;
		3. neprobíhá a podle nejlepšího vědomí a znalostí Dodavatele ani nehrozí žádné soudní, správní, rozhodčí ani jiné řízení či jednání před jakýmkoliv orgánem jakékoliv jurisdikce, které by mohlo, jednotlivě nebo v souhrnu s dalšími okolnostmi, nepříznivým způsobem ovlivnit schopnost Dodavatele splnit jeho závazky podle této Smlouvy;
		4. Dodavatel udržuje v platnosti ve všech zásadních ohledech licence, souhlasy, povolení a další oprávnění požadovaná právními předpisy platnými pro poskytnutí plnění dle Smlouvy a musí předcházet situaci, kdy by platnost takové licence, souhlasu, povolení a oprávnění byla ukončena. Plnění a jeho poskytnutí Objednateli nesmí být v rozporu s jakýmkoli právem třetí osoby na patentovou, známkoprávní, či jinou ochranu duševního vlastnictví, obchodní firmy či hospodářské soutěže;
		5. není si s vynaložením odborné péče vědom žádné překážky, týkající se Předmětu plnění (jak je tento pojem definován v čl. 2 odst. 2.1 této Smlouvy), nebo místa či prostředí Objednatele, která by znemožňovala nebo znesnadňovala poskytnout plnění způsobem sjednaným podle Smlouvy;
		6. v okamžiku dodání Předmětu plnění (jak je tento pojem definován v čl. 2 odst. 2.1 této Smlouvy) na základě Smlouvy je výlučným vlastníkem hmotných složek Předmětu plnění a není jakkoliv smluvně či zákonně omezen v dispozici s hmotnými složkami Předmětu plnění, jeho nabývací právní tituly k hmotným složkám Předmětu plnění jsou platné, účinné a vymahatelné, a že je oprávněn převést bez dalšího vlastnické právo k hmotným složkám Předmětu plnění na Objednatele, že neuzavřel ohledně hmotných složek Předmětu plnění žádnou smlouvu, kterou by převáděl na jinou osobu vlastnická nebo jiná práva k hmotným složkám Předmětu plnění, ani smlouvu o smlouvě budoucí obsahující závazek k budoucímu převodu hmotných složek Předmětu plnění;
		7. hmotné složky Předmětu plnění nejsou zatíženy zástavními, předkupními, nájemními či jinými právy třetích osob, jinými věcnými právy ani jinými omezeními;
		8. žádná třetí osoba nevznesla nárok, v jehož důsledku by mohlo dojít k omezení práva Dodavatele hmotné složky Předmětu plnění převést na Objednatele;
		9. Smlouva představuje platný a právně závazný závazek Dodavatele, který je vůči Dodavateli vynutitelný v souladu s podmínkami Smlouvy;
		10. Dodavateli není známa žádná skutečnost, okolnost či událost, která by měla za následek nebo by mohla mít za následek absolutní či relativní neplatnost Smlouvy.
	1. Dodavatel se zavazuje zajistit, aby jeho prohlášení dle této Smlouvy zůstala pravdivá

a v platnosti po celou dobu účinnosti Smlouvy.

* 1. Předmět plnění dle této Smlouvy bude poskytován prostřednictvím pracovníků Dodavatele, kteří jsou k tomu odborně kvalifikovaní.
	2. Veškeré ve Smlouvě uvedené požadavky musí být primárně vykládány tak, aby Objednatel realizací plnění ze strany Dodavatele dosáhl účelu uvedeného v odst. 1.1 tohoto článku Smlouvy.
	3. Dodavatel se zavazuje, že při realizaci Předmětu plnění dle této Smlouvy bude respektovat požadavky a zadání Objednatele do té míry, pokud tím nebudou porušeny zákonné předpisy nebo nebude toto jednání v rozporu s dobrými mravy.
	4. Dodavatel se zavazuje při realizaci Předmětu plnění dle této Smlouvy respektovat a dodržovat podmínky uvedené v Příloze č. 6 této Smlouvy.
	5. Hovoří-li se v přílohách této Smlouvy o zadavateli, rozumí se jím Objednatel.

##### Předmět Smlouvy

* 1. Předmětem této Smlouvy jsou následující závazky Dodavatele:
		1. dodávka GIS Systému v následujícím rozsahu včetně dodání příslušných SW licencí:
			1. ETL komponenta,
			2. Administrační komponenta ETL,
			3. Publikační komponenta,
			4. Mapová komponenta,
			5. Datová komponenta,

to vše včetně instalace, integrace do prostředí ISSI (implementace), základního nastavení, ověření funkčnosti (tyto služby dále jen „**Implementace**“)

(dále souhrnně jen „**GIS Systém**“, vlastní software dále jen „**Software**“ a licence

k němu poskytnuté dále jen „**Licence SW**“)

Bližší specifikace a technické požadavky na GIS Systém jsou uvedeny v Příloze č.

1 této Smlouvy a následujících ustanoveních této Smlouvy.

* + 1. poskytnutí školicích služeb spočívajících v zaškolení zaměstnanců Objednatele dle podmínek uvedených v odst. 2.6 tohoto článku a v následujících ustanoveních této Smlouvy (dále jen „**Školení**“)

(GIS Systém a Školení dále dohromady též jen jako „**Předmět plnění**“)

Pro vyloučení pochybností Objednatel stanovuje, že součástí Předmětu plnění dle písm. a) tohoto odstavce Smlouvy je taktéž Dokumentace dle odst. 2.2 tohoto článku Smlouvy a další dokumentace dle odst. 2.4 tohoto článku Smlouvy.

* 1. Součástí dodávky a ceny za GIS Systém bude následující dokumentace zpracovaná

v českém jazyce v editovatelné elektronické podobě:

1. **vývojová dokumentace** zahrnující komentáře ve zdrojovém kódu, celkový popis propojenosti jednotlivých SW částí (architektura), popis komunikačních rozhraních a jejich definici;
2. **administrátorská dokumentace** obsahující popis správy a implementace dodaných SW částí, popis logů a jejich struktura, metodiku odstraňování provozních chyb a problémů;
3. **uživatelská dokumentace** obsahující popis ovládání GIS Systému (srozumitelný návod na obsluhu systému a podrobný popis provádění jednotlivých úkonů), zejména grafických uživatelských rozhraní, popis procesů v GIS Systému;
4. **systémová dokumentace** obsahující popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností; podrobný popis GIS Systému nebo odkaz na dokument, ve kterém je popis uveden a který je Objednateli dostupný;
5. **dokumentace k řešení GIS Systému**, a to včetně identifikovaných datových toků, protokolů, architektonického nákresu komponent a jejich spolupráce, diagram logického a fyzického zapojení

(vše dohromady dále jen „**Dokumentace**“).

Objednatel se zavazuje bez zbytečného odkladu po písemné výzvě Dodavatele poskytnout nezbytně nutnou součinnost za účelem zpracování Dokumentace.

* 1. Veškerá Dokumentace bude zpracovaná v souladu s požadavky zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, a v souladu s vyhláškou č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy), ve znění pozdějších předpisů.
	2. Dokumentace podle odst. 2.2 tohoto článku Smlouvy, případně další dokumentace, jež je obvyklá, nutná (právními předpisy vyžadovaná) či vhodná k převzetí a k užívání GIS Systému, jako např. veškeré návody (manuály) k použití, záruční listy, funkční specifikace, doklady a dokumenty (např. prohlášení o shodě, licenční podmínky), bude Objednateli předána ve formátu PDF a DOC spolu s předáním Předmětu plnění do akceptačního řízení dle čl. 4 odst. 4.2 této Smlouvy. Hmotné nosiče, na nichž je Dokumentace zaznamenána, se okamžikem jejich předání Objednateli stávají jeho výlučným vlastnictvím. Veškerá tato další dokumentace dle tohoto odstavce Smlouvy bude v českém jazyce a okamžikem jejího předání Objednateli se stávají jeho výlučným vlastnictvím. Objednatel připouští také dodání uvedených dokumentů v anglickém jazyce vyjma licenčních podmínek, které budou vždy dodávány výhradně v českém jazyce.
	3. Dodavatel se zavazuje aktualizovat veškerou Dokumentaci, a případnou další dokumentaci podle odst. 2.4 tohoto článku Smlouvy, po celou dobu trvání této Smlouvy. Smluvní strany pro vyloučení případných nejasností sjednávají,

že aktualizace Dokumentace, a případné další dokumentace podle odst. 2.4 tohoto článku Smlouvy, po dobu trvání této Smlouvy je zahrnuta v Ceně (jak je tento pojem definován v čl. 5 odst. 5.2 této Smlouvy).

* 1. Školení dle odst. 2.1 písm. b) tohoto článku Smlouvy bude zahrnovat odborné proškolení určených zaměstnanců Objednatele. Školení bude probíhat v prostorách Objednatele nebo on-line, dle pokynu Objednatele. Účelem školení je seznámení určených zaměstnanců NAKIT s implementovaným GIS Systémem a jeho funkčností, a to minimálně v následujícím rozsahu:
		1. Administrátorské školení – školení v rozsahu tři (3) MD školení (jak je tento pojem definován v čl. 5 odst. 5.9 této Smlouvy) na základě administrátorské dokumentace i s názornými ukázkami např. odstraňování provozních chyb a problémů, čtení logů a jejich vyhodnocování, nastavování SW apod;
		2. Uživatelské školení – školení v rozsahu tři (3) MD školení na základě uživatelské dokumentace, praktické ukázky práce s GIS Systémem a implementovanými procesy.

Pro vyloučení pochybností se stanoví, že MD školení je MD strávený aktivním školením uživatelů/administrátorů. Cena za MD školení zahrnuje veškeré náklady dodavatele na přípravu a realizaci školení, zejm. pak vypracování osnov a školících manuálů pro oba typy Školení na obsluhu systému pro jeho využití a na administraci a jejich předání Objednateli v počtu dvou (2) ks výtisků a v elektronické podobě na vhodném datovém nosiči v počtu jednoho (1) ks ve formátu PDF a současně v otevřeném formátu Microsoft Office (např. Word, Excel apod.). Dodavatel tedy není oprávněn požadovat úhradu nákladů spojených s přípravou či realizací školení nad rámec ceny za MD školení.

Organizace Školení bude plně v kompetenci Dodavatele, Školení však musí být provedeno nejpozději do pěti (5) pracovních dnů do doby ukončení akceptačního řízení dle čl. 4 odst. 4.2 této Smlouvy.

* 1. Dodavatel se zavazuje poskytnout Objednateli Předmět plnění v souladu s touto Smlouvou, tedy ve sjednaném rozsahu, kvalitě a čase.
	2. Objednatel se zavazuje řádně a včas provedený Předmět plnění v souladu s podmínkami této Smlouvy převzít a zaplatit za něj Dodavateli sjednanou Cenu.
	3. Po uzavření Smlouvy odešle Objednatel Dodavateli číslo tzv. Evidenční objednávky (EOBJ), která má pouze evidenční charakter pro Objednatele a nemá žádný vliv na plnění Smlouvy. Číslo EOBJ je Dodavatel povinen uvádět na daňových dokladech (viz čl. 6 odst. 6.2 této Smlouvy). Neuvedení čísla EOBJ na faktuře je důvodem k neproplacení faktury a jejímu oprávněnému vrácení Dodavateli ve smyslu ustanovení čl. 6 odst. 6.3 této Smlouvy.
	4. Smluvní strany sjednávají, že dojde-li ze strany Dodavatele v rámci plnění předmětu této Smlouvy k updatům, legislativním updatům, upgradům, legislativním upgradům, mimořádným updatům a/nebo patchům GIS Systému, jak jsou tyto definovány níže v tomto odstavci pod body a) až e), budou tyto updaty, legislativní updaty, upgrady a legislativní upgrady, mimořádné updaty a patche GIS Systému zahrnuty do Ceny a Dodavateli za jejich provedení nebude náležet žádná další odměna.
		1. pod pojmem **update** se v této Smlouvě rozumí taková verze GIS Systému nebo jeho části, u které se oproti předcházející verzi GIS Systému mění jeho funkčnost, a to na základě změny jakékoliv skutečnosti, podle které byla celá funkčnost GIS Systému vytvořena, ale nemění se struktura dat datového fondu, se kterým tato verze GIS Systému pracuje. V případě, že změna funkčnosti GIS Systému byla provedena pouze na základě legislativních změn, je nová verze GIS Systému jeho “**legislativním updatem**”,
		2. pod pojmem **upgrade** se ve Smlouvě rozumí taková verze GIS Systému nebo jeho části, u které se oproti předcházející verzi GIS Systému mění jeho funkčnost, a to na základě změny jakékoliv skutečnosti, podle které byla celá funkčnost GIS Systému vytvořena, a zároveň se mění struktura vět datového fondu, se kterým tato verze GIS Systému pracuje. V případě, že změna funkčnosti GIS Systému a změna struktury dat datového fondu, se kterým GIS Systému pracuje, byla provedena pouze na základě legislativních změn, je nová verze GIS Systému jeho “**legislativním upgradem**”,
		3. pod pojmem „**patch“** se ve Smlouvě rozumí sada změn provedených v programu, anebo datech (update) určených k aktualizaci, opravě anebo vylepšení, a to obvykle prostřednictvím opravného balíčku. Provedená sada změn zahrnuje většinou opravu bezpečnostních anebo jiných chyb, a vede ke zlepšení bezpečnosti, výkonu či funkčnosti programu,
		4. ke každé verzi GIS Systému po updatu, upgradu, legislativním updatu, legislativním upgradu, mimořádném updatu a patchi dle této Smlouvy je Dodavatel povinen dodat seznam změn a úprav v elektronické formě, které byly provedeny do inovované verze. Budou-li inovované verze obsahovat modifikovanou funkčnost oproti předchozí verzi, potom budou tyto Dodavatelem distribuovány Objednateli spolu s náležitou Dokumentací v elektronické podobě na vhodném datovém nosiči v počtu dvou (2) kusů ve formátu PDF a současně i MS Word a MS Excel. V případě požadavku ze strany Objednatele je Dodavatel povinen zajistit školení s ohledem na dopady, které změny inovované verze GIS Systému vyvolaly/vyvolají.
		5. Dodavatel je povinen na písemné vyžádání Objednatele opatřit GIS Systém

a každý update, legislativní update, upgrade a legislativní upgrade, mimořádný

update a patch GIS Systému čestným prohlášením o tom, že GIS Systém, případně provedený update či upgrade, je ve shodě s platnými právními předpisy České republiky.

* 1. Pod pojmem „**jednotka“**, jak je tento pojem použit v cenové specifikaci uvedené v Příloze č. 2 této Smlouvy, se rozumí jedna samostatně spuštěná komponenta ve smyslu a rozsahu dle Přílohy č. 1 této Smlouvy.
	2. Dodavatel se zavazuje poskytnout Objednateli oprávnění ve smyslu čl. 7 této Smlouvy a Příloh č. 1 a 5 této Smlouvy (Licence SW) k odpovídajícímu počtu jednotek (jak je tento pojem definován v odst. 2.11 tohoto článku Smlouvy) Software uvedenému v Příloze č. 2 této Smlouvy pro účel a rozsah využití specifikovaný touto Smlouvou a Přílohou č. 1 této Smlouvy.

##### Doba, místo a podmínky poskytování Předmětu plnění

* 1. Předmět plnění dle čl. 2 odst. 2.1 této Smlouvy bude Dodavatelem dodán do šesti (6) měsíců od podpisu této Smlouvy, nejpozději však do 31. 10. 2022. V případě, že k uzavření této Smlouvy dojde po dni 1. 5. 2022, prodlužuje se termín pro dodání Předmětu plnění o stejný počet kalendářních dnů, o který byla tato Smlouva uzavřena později oproti dni 1. 5. 2022. Prodloužení termínu podle předchozí věty se nepoužije, pokud Dodavatel při podpisu této Smlouvy písemně prohlásí, že dodrží termín plnění
1. 10. 2022. S ohledem na to, že v případě splnění po datu 31. 10. 2022 nemá Objednatel postaveno na jisto, že využije Předmět plnění a že má pro Předmět plnění zajištěno financování, Objednatel si v souvislosti s ujednáním v tomto odstavci Smlouvy vyhrazuje, že pro případ, kdy by měl být předmět této Smlouvy splněn až po dni 31. 10. 2022 má Objednatel právo odstoupit od této Smlouvy v souladu s čl. 17 odst. 17.4 této Smlouvy, a to ve lhůtě deseti (10) kalendářních dnů ode dne podpisu této Smlouvy. V takovém případě nemá Dodavatel právo na jakékoli plnění ze strany Objednatele.
	1. Dnem dodání Předmětu plnění se pro účely této Smlouvy rozumí den podpisu Akceptačního protokolu (jak je tento pojem definován v čl. 4 odst. 4.2 této Smlouvy) Objednatelem s výrokem „Akceptováno“ nebo „Akceptováno s výhradou“.
	2. Místem plnění je Česká republika.
	3. Termín a místo Předmětu plnění dle odst. 3.1 a 3.3 tohoto článku Smlouvy lze změnit jen s výslovným a předchozím souhlasem Smluvních stran.
	4. Dodavatel se zavazuje alokovat na poskytování služeb Implementace a Školení dle čl. 2 odst. 2.1 této Smlouvy kapacity osob s kompetencemi dostatečnými k poskytování

těchto služeb. Dodavatel je povinen zajistit kontinuitu svých osob podílejících se na plnění dle této Smlouvy dle předchozí věty v celém průběhu plnění předmětu Smlouvy.

Objednatel si vyhrazuje právo písemně požádat Dodavatele o výměnu člena realizačního týmu pro opakovanou nespokojenost s kvalitou jím odváděné práce nebo pro nedostatečnou komunikaci s Objednatelem. Pokud Objednatel požádá o výměnu člena realizačního týmu, není Dodavatel oprávněn plnit prostřednictvím osoby, o jejíž výměnu Objednatel požádal, své závazky.

Smluvní strany pro vyloučení případných pochybností sjednávají, že v případě nahrazení člena realizačního týmu novým členem není nutné k této Smlouvě uzavírat dodatek.

Dodavatel je dále povinen zajistit, aby členové realizačního týmu byli řádně a prokazatelně proškoleni v oblasti bezpečnosti dat a informací.

* 1. Dodavatel není oprávněn postoupit ani převést jakákoliv svá práva či povinnosti vyplývající ze Smlouvy bez předchozího písemného souhlasu Objednatele na třetí osoby. Dodavatel je oprávněn pověřit plněním závazků plynoucích ze Smlouvy jiné třetí osoby (poddodavatele), nebo takové třetí osoby (poddodavatele) změnit, uvedl-li je již ve své nabídce v Zadávacím řízení (dále jen „**Nabídka**“), pouze s předchozím písemným souhlasem Objednatele. Pokud se jedná o takové třetí osoby (poddodavatele), kterými Dodavatel prokazoval kvalifikaci, tak musí tato nová třetí osoba (poddodavatel) splňovat kvalifikační předpoklady minimálně v rozsahu stanoveném v Zadávacím řízení. Pokud byla tato třetí osoba (poddodavatel) taktéž součástí hodnocení nabídek v Zadávacím řízení, tak musí taktéž splňovat kvalifikační předpoklady minimálně v takovém rozsahu, v jakém byly započteny do tohoto hodnocení nabídek v Zadávacím řízení u původní třetí osoby (poddodavatele). Dodavatel je povinen splnění náležitostí dle předchozí věty doložit před odsouhlasením této změny Objednatelem, a to stejnou formou, jaká byla vyžadována v Zadávacím řízení. Udělí-li Objednatel s využitím nebo změnou třetí osoby (poddodavatele) souhlas, je Dodavatel povinen zavázat poddodavatele k zachování důvěrných informací a k ochraně osobních údajů ve smyslu čl. 10 a 11 této Smlouvy a k zajištění bezpečnostních požadavků zejména ve smyslu čl. 16 této Smlouvy ve stejném rozsahu, v jakém je k této povinnosti zavázán sám. Dodavatel odpovídá za své poddodavatele jako za plnění vlastní, včetně odpovědnosti za způsobenou újmu. Dodavatel se zavazuje neprodleně doložit Objednateli na základě jeho výzvy smluvní dokumenty se svými poddodavateli, ze kterých bude vyplývat závazek poddodavatele poskytovat plnění v souladu s požadavky na ochranu důvěrných informací a osobních údajů a bezpečnostními požadavky vyplývajícími z této Smlouvy.
	2. Dodavatel je povinen zajistit, že i jeho poddodavatelé, kteří se budou podílet na plnění této Smlouvy, se zaváží dodržovat v plném rozsahu ujednání mezi Dodavatelem a

Objednatelem a nebudou v rozporu s požadavky Objednatele uvedenými v této Smlouvě.

* 1. Objednatel tímto sděluje Dodavateli a Dodavatel podpisem této Smlouvy souhlasí s tím, že příjemcem plnění poskytnutého na základě této Smlouvy může být kromě Objednatele také Koncový zákazník.
	2. Služba Implementace dle čl. 2 odst. 2.1 písm. a) této Smlouvy bude probíhat v souladu s požadavky uvedenými v Příloze č. 1 Smlouvy.

##### Akceptační řízení

* 1. Akceptační řízení u Předmětu plnění dle čl. 2 odst. 2.1 písm. a) této Smlouvy zahrnuje ověření řádného provedení Předmětu plnění porovnáním skutečných vlastností Předmětu plnění s jeho specifikací stanovenou touto Smlouvou. Základní požadavky na akceptační kritéria pro Předmět plnění dle čl. 2 odst. 2.1 písm. a) této Smlouvy vyplývají z technických a funkčních požadavků uvedených v Příloze č. 1 této Smlouvy. Dodavatel povinen do šedesáti (60) kalendářních dnů od uzavření této Smlouvy zaslat Objednateli návrh struktury akceptačních testů pro Předmět plnění dle čl. 2 odst. 2.1 písm. a) této Smlouvy, a to za dodržení všech technických a funkčních požadavků vyplývajících z této Smlouvy a její Přílohy č. 1 (dále jen „**Návrh akceptačních testů**“). Objednatel následně ve lhůtě čtrnácti (14) kalendářních dnů Dodavatele informuje, zda s Návrhem akceptačních testů návrhem souhlasí či nikoliv. V případě, že Objednatel nebude s Návrhem akceptačních testů souhlasit, zavazují se Smluvní strany svolat jednání s cílem nastavení podmínek akceptačních testů.
	2. Akceptační řízení je zahájeno dnem předání Předmětu plnění (tzn. předáním naimplementovaného GIS Systému) vč. aktuálních verzí Dokumentace a případné další dokumentace dle čl. 2 odst. 2.4 této Smlouvy Dodavatelem do akceptačního řízení a je ukončeno podpisem akceptačního protokolu oběma Smluvními stranami (dále jen „**Akceptační protokol**“) s výrokem „Akceptováno“ nebo „Akceptováno s výhradou“. Provedením zkušebního provozu Předmětu plnění a akceptačních testů Předmětu plnění Dodavatel prokáže a Objednatel ověří, že Předmět plnění je provedeno kvalitně, odborně a plní veškeré požadované funkcionality.
	3. Nestanoví-li Objednatel jinak, bude nedílnou součástí Akceptačního protokolu taktéž:
		1. Prohlášení Dodavatele, že ke dni akceptace jsou způsobem určeným dle této Smlouvy předány Objednateli aktuální verze zdrojových kódů včetně aktuální verze veškeré související dokumentace, bude-li Dodavatel povinen tyto zdrojové kódy a související dokumentaci v souladu s touto Smlouvou poskytnout;
		2. jakékoli další materiály vztahující se k předmětnému Předmětu plnění.

Dokumentace předaná současně s Předmětem plnění do akceptačního řízení podléhá rovněž akceptačnímu řízení. Veškerá Dokumentace a případná další dokumentace dle čl. 2 odst. 2.4 této Smlouvy se stává výlučným vlastnictvím Objednatele dnem podpisu Akceptačního protokolu.

* 1. V případě výskytu vad a nedodělků bránících řádnému užívání Předmětu plnění Objednatelem v termínu předání a převzetí nebude Předmět plnění převzat až do jejich odstranění. Pokud Objednatel Předmět plnění nepřevezme, protože obsahuje vady, je povinen specifikovat tyto vady v Akceptačním protokolu. Smluvní strany se písemně záznamem do Akceptačního protokolu dohodnou, do kdy Dodavatel odstraní tyto vady Předmětu plnění tak, aby byla splněna všechna kritéria funkčnosti Předmětu plnění. Do odstranění těchto vad není Objednatel povinen Akceptační protokol podepsat a zaplatit cenu Předmětu plnění. V případě, že se u Předmětu plnění vyskytují méně závažné vady, které nebrání jeho řádnému užívání, může Objednatel převzít tento Předmět lnění i s těmito vadami, které je povinen specifikovat v Akceptačním protokolu. Pokud Objednatel převezme Předmět plnění s vadami dle předchozí věty, tj. podepíše Akceptační protokol s výrokem „Akceptováno s výhradou“, zavazuje se Dodavatel vady specifikované v Akceptačním protokolu odstranit bez zbytečného odkladu, nejpozději však do deseti (10) pracovních dnů, nestanoví-li Objednatel lhůtu delší.
	2. V Akceptačním protokolu bude stanoven harmonogram Školení dle čl. 2 odst. 2.1 písm.

b) a odst. 2.6 této Smlouvy.

* 1. Akceptační protokol bude vyhotoven ve dvou (2) vyhotoveních a podepsán oběma Smluvními stranami. Každá ze Smluvních stran obdrží po jednom (1) vyhotovení.
	2. Podpisem Akceptačního protokolu s výrokem „Akceptováno“ nebo „Akceptováno s výhradou“ oběma Smluvními stranami se má za to, že je splněn závazek Dodavatele dle této Smlouvy provést Předmět plnění a Dodavateli vzniká právo na zaplacení příslušné ceny za Předmět plnění.
	3. Smluvní strany sjednávají, že k podpisu všech akceptačních dokumentů uvedených

v tomto článku Smlouvy jsou oprávněny osoby uvedené v Příloze č. 4 této Smlouvy.

* 1. Vzor Akceptačního protokolu je uveden v Příloze č. 3 této Smlouvy. Smluvní strany pro vyloučení případných nejasností sjednávají, že vzor Akceptačního protokolu může být upravován.

##### Cena

* 1. Jednotkové ceny pro jednotlivé položky Předmětu plnění jsou uvedeny v Příloze č. 2 této Smlouvy a vycházejí z jednotkových cen uvedených v Nabídce. Jednotkové ceny jsou konečné a nejvýše přípustné a jsou v nich zahrnuty veškeré náklady Dodavatele

související s plněním Smlouvy a poskytnutím Předmětu plnění Objednateli. Dodavatel tímto Objednateli zaručuje úplnost cen plnění uvedených v Příloze č. 2 této Smlouvy.

* 1. Cena za dodávku Předmětu plnění dle čl. 2 odst. 2.1 této Smlouvy je stanovena dle Nabídky a činí **7 891 848,00 Kč** bez DPH (slovy: sedm milionů osm set devadesát jeden tisíc osm set čtyřicet osm korun českých) (dále jen „**Cena**“).
	2. V jednotkových cenách Licencí SW jsou zahrnuty zejména:
		1. instalační média se Software a jejich doprava do místa určeného Objednatelem (pokud je Software distribuován ve formě hmotných nosičů, případně zpřístupnění instalačních dat k Software přes internet);
		2. clo, celní poplatky, daně (vyjma DPH, která bude připočtena podle odst. 5.8 tohoto článku Smlouvy) a zálohy;
		3. recyklační poplatky a ekologická likvidace instalačních médií (pokud probíhá distribuce Software formou instalačních médií) a činnosti s ní spojené;
		4. veškeré jiné náklady a poplatky nezbytné pro řádné plnění Smlouvy.
	3. Objednatel si v souladu se zadávací dokumentací k Zadávacímu řízení (dále jen

„**Zadávací dokumentace**“) a § 222 odst. 2 ZZVZ vyhrazuje možnost změny závazku ze Smlouvy, a to:

* + 1. navýšením Ceny z důvodu potřeby Objednatele navýšit počet Licencí SW k Software v důsledku zvýšení parametrů využití Software (parametrů běhového systému).

Objednatel předpokládá provoz GIS Systému dle parametrů běhového systému definovaných v čl. 5 Přílohy č. 1 této Smlouvy. Důvodem pro potřebu navýšit počet Licencí SW je změna těchto parametrů běhového prostředí, která ovlivní počet a strukturu Licencí SW v dosavadním licenčním modelu poskytovaném Dodavatelem (z hlediska cen licencí SW dodavatele i SW třetích stran, jak je uvedeno v Příloze č. 2 této Smlouvy, v listu „detail“). V případě navýšení počtu Licencí SW ve smyslu tohoto odstavce Smlouvy dojde k navýšení Ceny, a to o částku odpovídající součinu počtu jednotlivých položek Licencí SW potřebných k provozování systému, o které se celkový počet položek Licencí SW navyšuje a jednotkových cen těchto jednotlivých položek Licencí SW stanovených v Příloze č. 2 této Smlouvy (list „detail").

* + 1. snížením Ceny z důvodu potřeby Objednatele disponovat nižším počtem Licencí SW k Software v důsledku snížení parametrů využití Software (parametrů běhového systému).

Objednatel předpokládá provoz GIS Systému dle parametrů běhového systému definovaných v čl. 5 Přílohy č. 1 této Smlouvy. Důvodem pro potřebu snížit počet

Licencí SW je změna těchto parametrů běhového prostředí, která ovlivní počet a strukturu Licencí SW v dosavadním licenčním modelu poskytovaném Dodavatelem (z hlediska cen licencí SW dodavatele i SW třetích stran, jak je uvedeno v Příloze č. 2 této Smlouvy, v listu „detail“). V případě snížení počtu Licencí SW ve smyslu tohoto odstavce Smlouvy dojde ke snížení Ceny, a to o částku odpovídající součinu počtu jednotlivých položek Licencí SW, které zadavatel pro provozování systému nepotřebuje a jejichž počet tedy chce snížit a jednotkových cen těchto jednotlivých položek Licencí SW stanovených v Příloze č. 2 této Smlouvy (list „detail").

Dodavatel bere uvedenou vyhrazenou změnu závazku na vědomí a toto stvrzuje podpisem této Smlouvy. Ke změně cen za užívání licencí podle tohoto odstavce Smlouvy dojde dodatkem k této Smlouvě. Objednatel má právo zajistit změny v počtu licencí i od třetích osob. Pro vyloučení pochybností se stanoví, že pojem

„počet licencí“ zahrnuje jakékoli navýšení či snížení ceny za licenci, pokud jsou vyvolány změnami prostředí uvedenými v písmenech a) nebo b) tohoto odstavce Smlouvy, i když jednotka změny není označována jako „počet licencí“.

* 1. V případě potřeby zvýšení nebo snížení počtu Licencí SW dle odst. 5.4 tohoto článku Smlouvy nad původní počet uvedený v Zadávací dokumentaci, zašle Objednatel Dodavateli písemný návrh na uzavření dodatku, který bude obsahovat zejména:
		1. specifikaci a počet požadovaných Licencí SW,
		2. termín poskytnutí Licencí SW,
		3. jednotkovou a celkovou cenu, přičemž tyto ceny budou stanoveny dle jednotkových cen uvedených v Příloze č. 2 této Smlouvy,

(dále jen „**Návrh**“)

* 1. Dodavatel je následně povinen Návrh posoudit a pokud není v rozporu s touto Smlouvou, je povinen jej písemně akceptovat ve lhůtě pěti (5) pracovních dnů od jeho doručení Objednatelem, pokud nebude Objednatelem stanovena lhůta delší. Ke změně Ceny za Licence SW podle tohoto odstavce Smlouvy dojde dodatkem k této Smlouvě a k poskytnutí těchto Licencí SW. Povinnost akceptovat Návrh se uplatní pouze pro Návrhy doručené v prvních 5 letech ode dne uzavření této smlouvy.
	2. Pro poskytování Licencí SW ve smyslu odst. 5.4 tohoto článku Smlouvy se přiměřeně použijí příslušná ustanovení této Smlouvy.
	3. Veškeré ceny jsou uvedeny v Kč bez daně z přidané hodnoty (dále jen „**DPH**“). K Ceně bude připočítána DPH dle příslušných předpisů ve výši platné ke dni uskutečnění zdanitelného plnění.
	4. Jedním člověkodnem (dále jen „**MD**“) se pro účely této Smlouvy rozumí součet osmi

(8) člověkohodin poskytovaných služeb, které nemusí být poskytovány ve stejný den. Členové realizačního týmu budou evidovat svoji práci s přesností na dokončenou půlhodinu, která je nejmenší samostatně rozlišitelnou jednotkou.

##### Platební a fakturační podmínky

* 1. Daňový doklad (fakturu) za Předmět plnění podle čl. 2 odst. 2.1 této Smlouvy je Dodavatel oprávněn vystavit po podepsání Akceptačního protokolu dle čl. 4 odst.

4.2 této Smlouvy oběma Smluvními stranami. Za den uskutečnění zdanitelného plnění se považuje den podpisu Akceptačního protokolu Objednatelem, který bude přílohou daňového dokladu.

* 1. Daňový doklad (faktura) vystavený Dodavatelem musí obsahovat náležitosti řádného daňového dokladu podle příslušných právních předpisů, zejména dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**zákon o DPH**“), a zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zejména tyto údaje:
		+ identifikační údaje Objednatele a Dodavatele,
		+ číslo Smlouvy,
		+ číslo Evidenční objednávky (EOBJ) – viz čl. 2 odst. 2.9 této Smlouvy,
		+ popis fakturovaného plnění, rozsah, jednotkovou a celkovou cenu,
		+ platební podmínky v souladu se Smlouvou,
		+ přílohou daňového dokladu je vždy kopie Akceptačního protokolu podepsaného oběma Smluvními stranami.
	2. V případě, že daňový doklad nebude mít odpovídající náležitosti nebo nebude vystaven v souladu s touto Smlouvou, je Objednatel oprávněn jej ve lhůtě splatnosti zaslat zpět k doplnění Dodavateli, aniž se dostane do prodlení se splatností. Lhůta splatnosti třicet

(30) kalendářních dnů počíná běžet znovu od data doručení nově vystaveného/opraveného daňového dokladu Objednateli.

* 1. Splatnost daňového dokladu (faktury) vystaveného Dodavatelem je třicet (30) kalendářních dnů ode dne doručení Objednateli. Dodavatel zašle daňový doklad spolu s veškerými požadovanými dokumenty Objednateli do tří (3) pracovních dnů od jejich vystavení jedním z následujících způsobů:
1. v elektronické podobě na adresu: faktury@nakit.cz

nebo

1. doporučeným dopisem na následující adresu:

Národní agentura pro komunikační a informační technologie, s. p. Kodaňská 1441/46, Vršovice, 101 01 Praha10

* 1. Platba bude provedena v české měně formou bankovního převodu na účet Dodavatele uvedený v záhlaví této Smlouvy.
	2. Faktura se považuje za uhrazenou dnem odepsání příslušné finanční částky z účtu Objednatele ve prospěch účtu Dodavatele.
	3. Objednatel neposkytuje Dodavateli jakékoliv zálohy na cenu za Předmět plnění.
	4. Všechny částky poukazované vzájemně Smluvními stranami musí být prosté jakýchkoliv bankovních poplatků nebo jiných nákladů spojených s převodem na jejich účty.
	5. Smluvní strany si ve smyslu ust. § 2620 odst. 2 občanského zákoníku ujednaly, že Dodavatel na sebe přebírá nebezpečí změny okolností.
	6. Smluvní strany se dohodly, že pokud bude v okamžiku uskutečnění zdanitelného plnění správcem daně zveřejněna způsobem umožňujícím dálkový přístup skutečnost, že dodavatel zdanitelného plnění (Dodavatel) je nespolehlivým plátcem ve smyslu

§ 106a zákona o DPH, nebo má-li být platba za zdanitelné plnění uskutečněné Dodavatelem v tuzemsku zcela nebo z části poukázána na bankovní účet vedený poskytovatelem platebních služeb mimo tuzemsko, je příjemce zdanitelného plnění (Objednatel) oprávněn část ceny odpovídající dani z přidané hodnoty zaplatit přímo na bankovní účet správce daně ve smyslu § 109a zákona o DPH. Na bankovní účet Dodavatele bude v tomto případě uhrazena část ceny odpovídající výši základu daně z přidané hodnoty. Úhrada ceny plnění (základu daně) provedená Objednatelem v souladu s ustanovením tohoto odstavce Smlouvy bude považována za řádnou úhradu ceny plnění poskytnutého dle této Smlouvy.

Bankovní účet uvedený na daňovém dokladu, na který bude ze strany Dodavatele požadována úhrada ceny za poskytnuté zdanitelné plnění, musí být Dodavatelem zveřejněn způsobem umožňujícím dálkový přístup ve smyslu § 96 zákona o DPH. Smluvní strany se výslovně dohodly, že pokud číslo bankovního účtu Dodavatele, na který bude ze strany Dodavatele požadována úhrada ceny za poskytnuté zdanitelné plnění dle příslušného daňového dokladu, nebude zveřejněno způsobem umožňujícím dálkový přístup ve smyslu § 96 zákona o DPH a cena za poskytnuté zdanitelné plnění dle příslušného daňového dokladu přesahuje limit uvedený v § 109 odst. 2 písm. c) zákona o DPH, je Objednatel oprávněn zaslat daňový doklad zpět Dodavateli k opravě. V takovém případě se doba splatnosti zastavuje a nová doba splatnosti počíná běžet dnem doručení opraveného daňového dokladu Objednateli s uvedením správného bankovního účtu Dodavatele, tj. bankovního účtu zveřejněného správcem daně.

##### Licence a podmínky užití Předmětu plnění

* 1. Vzhledem k tomu, že součástí Předmětu plnění je i plnění, které může naplňovat znaky autorského díla ve smyslu AZ, jsou k těmto částem Předmětu plnění poskytována příslušná oprávnění (Licence SW) za podmínek sjednaných dále v tomto článku Smlouvy a v Příloze č. 1 této Smlouvy. V případě rozporu ustanovení Přílohy č. 1 s tímto článkem Smlouvy, má přednost tento článek Smlouvy, ledaže ustanovení Přílohy č. 1 této Smlouvy stanoví širší či výhodnější práva pro Objednatele.
	2. Objednatel je oprávněn veškeré součásti Předmětu plnění považované za autorské dílo ve smyslu AZ (dále jen „**Autorské dílo**“) užívat dle níže uvedených podmínek.
	3. Objednatel je oprávněn Autorské dílo užívat dle níže uvedených licenčních podmínek (Licence SW), a to od okamžiku účinnosti poskytnutí Licence SW, přičemž Dodavatel poskytuje Objednateli Licenci SW s účinností, která nastává okamžikem předání Předmětu plnění či jeho části, jehož je Autorské dílo součástí. Licence je udělena k užití Autorského díla Objednatelem k jakémukoliv účelu a v rozsahu, v jakém uzná na nezbytné, vhodné či přiměřené. Pro vyloučení všech pochybností to znamená, že:
		1. Licence SW je nevýhradní a neomezená, a to zejména ke splnění účelu Smlouvy (je-li Autorským dílem počítačový program, vztahuje se Licence SW ve stejném rozsahu na Autorské dílo ve strojovém i zdrojovém kódu, jakož i na koncepční přípravné materiály);
		2. Licence SW je bez časového (po dobu trvání majetkových práv autorských k příslušným Autorským dílům) a územního omezení a v množstevním rozsahu dle parametrů běhového prostředí definovaných v čl. 5 Přílohy č. 1 této Smlouvy s přihlédnutím k možné změně těchto parametrů v případě aplikace čl. 5 odst. 5.4 této Smlouvy, a pro všechny způsoby užití;
		3. Objednatel je oprávněn výsledky činnosti dle této Smlouvy (Autorská díla) užít v původní nebo jiným zpracované či jinak změněné podobě, samostatně nebo v souboru anebo ve spojení s jiným dílem či prvky;
		4. Licence SW je bez potřeby jakéhokoliv dalšího svolení Dodavatele udělena Objednateli s právem podlicence nebo je rovněž dále postupitelná jakékoliv třetí osobě;
		5. Licence SW se vztahuje automaticky i na všechny nové verze, úpravy a překlady příslušných Autorských děl;
		6. Dodavatel společně s Licencí SW poskytuje Objednateli právo provádět jakékoliv modifikace, úpravy, změny Autorského díla a dle svého uvážení do něj zasahovat,

zapracovávat ho do dalších Autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob;

* + 1. Licence SW není Objednatel povinen využít, a to ani zčásti;
		2. Licenční poplatek za výše uvedená oprávnění k příslušným Autorským dílům je zahrnut v Ceně dle čl. 5 odst. 5.2 této Smlouvy s přihlédnutím k účelu Licence SW a způsobu a okolnostem užití Autorských děl a k územnímu a časovému a množstevnímu rozsahu Licence SW.

Pro vyloučení pochybností Objednatel stanovuje, že shora uvedená Licence SW se vztahuje ve stejném rozsahu i na Dokumentaci dle čl. 2 odst. 2.2 a další dokumentaci dle čl. 2 odst. 2.4 této Smlouvy.

* 1. V souvislosti s poskytnutými oprávněními dle odst. 7.3 tohoto článku Smlouvy je Dodavatel povinen nejpozději v rámci akceptace (předání části Předmětu plnění do akceptačního řízení) Předmětu plnění dle této Smlouvy předat Objednateli zdrojový kód každé jednotlivé části Autorského díla, která je počítačovým programem, a která je Objednateli poskytována na základě Předmětu plnění, vyjma Proprietárního SW (jak je tento pojem definován v odst. 7.6 tohoto článku Smlouvy). Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručující možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující kompilaci, instalaci, spuštění a ověření funkcionality. Zdrojové kódy budou Objednateli Dodavatelem předány ve formě jejich nahrání do repozitáře Git – konkrétně do Azure Devops Objednatele, a to včetně instalačních souborů, struktury a popisu databáze, administrátorské, vývojové, bezpečnostní a provozní dokumentace a uživatelské dokumentace. O předání / nahrání zdrojových kódů bude oběma Smluvními stranami podepsán předávací protokol.
	2. Povinnost Dodavatele uvedená v odst. 7.4 tohoto článku Smlouvy se použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update zdrojového kódu každé jednotlivé části Autorského díla, která je počítačovým programem, k nimž dojde (i) při plnění této Smlouvy nebo (ii) v rámci oprav dle záruky dle této Smlouvy nebo (iii) v rámci úprav při poskytování služby podpory, kterou bude Dodavatel zajišťovat v rámci plnění smlouvy s názvem Podpora ke GIS Systému, která je taktéž uzavřena s tentýž dodavatelem na základě výsledku Zadávacího řízení, (iv) nebo v rámci rozvojových a konfiguračních prací, které budou provádět osoby určené Dodavatelem v rámci plnění smlouvy s názvem Rámcová dohoda na poskytování integračních a konfiguračních služeb, která je taktéž uzavřena s tentýž dodavatelem na základě výsledku Zadávacího řízení (dále jen „**Změna zdrojového kódu**“). Dokumentace Změny zdrojového kódu musí obsahovat podrobný popis a komentář každého zásahu do zdrojového kódu.
	3. Součástí plnění dle této Smlouvy může být tzv. proprietární SW, u kterého Dodavatel nemůže Objednateli poskytnutou oprávnění dle odst. 7.3 tohoto článku Smlouvy nebo

to po něm nelze spravedlivě požadovat, avšak pouze za splnění některé

z následujících podmínek:

* + 1. jedná se o SW subjektů, jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi na sobě nezávislými a vzájemně nepropojenými subjekty oprávněnými takový SW distribuovat a který je v době uzavření této Smlouvy prokazatelně používán v produktivním prostředí nejméně u deseti na sobě nezávislých a vzájemně nepropojených subjektů. Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat;
		2. jedná se o SW, u kterého Dodavatel poskytne s ohledem na jeho (i) nekomplikovanou propojitelnost či (ii) oddělitelnost a nahraditelnost v rámci plnění předmětu této Smlouvy bez nutnosti vynakládání výraznějších prostředků, písemnou garanci, že další rozvoj Předmětu plnění jinou osobou než Dodavatelem je možné provádět bez toho, aby tím byla dotčena práva autorů takového SW, neboť nebude nutné zasahovat do zdrojových kódů takového SW anebo proto, že případné nahrazení takového SW nebude představovat výraznější komplikaci a náklad na straně Objednatele.
		3. Dodavatel Objednateli k SW poskytne nebo zprostředkuje poskytnutí úplných komentovaných zdrojových kódů SW a bezpodmínečného práva provádět jakékoliv modifikace, úpravy, změny takového SW a dle svého uvážení do něj zasahovat, zapracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob. Poskytování zdrojových kódů se řídí odst. 7.4 a 7.5 tohoto článku Smlouvy.

(dále jen „**Proprietární SW**“).

* 1. U Proprietárního SW postačí, aby Objednatel nabyl k Proprietárnímu SW nevýhradní oprávnění užít jej jakýmkoli způsobem bez časového a územního omezení a v množstevním rozsahu dostatečném k užívání v rozsahu dle této Smlouvy, zejména dle parametrů běhového prostředí definovaných v čl. 5 Přílohy č. 1 této Smlouvy s přihlédnutím k možné změně těchto parametrů v případě aplikace čl. 5 odst. 5.4 této Smlouvy, a to včetně práva Objednatele do Proprietárního SW zasahovat, pokud tak stanoví příslušné ustanovení odst. 7.6 písm. a), b) či c) tohoto článku Smlouvy (nelze- li to na Dodavateli spravedlivě požadovat a není-li to v rozporu s ustanoveními odst.

7.6 písm. a), b) či c) tohoto článku Smlouvy, nemusí být Objednateli k Proprietárnímu SW předány zdrojové kódy a stejně nemusí být poskytnuto právo Objednatele do Proprietárního SW zasahovat, vždy však musí být předána kompletní uživatelská, administrátorská a provozní dokumentace). Dodavatel je povinen samostatně zdokumentovat veškeré využití Proprietárního SW v rámci Předmětu plnění a předložit v rámci Nabídky Objednateli ucelený přehled využitého Proprietárního SW, jeho

licenčních podmínek a alternativních dodavatelů. Tato specifikace Proprietárního SW je uvedena v Příloze č. 5 této Smlouvy.

* 1. Je-li součástí Předmětu plnění tzv. **open source SW**, u kterého Dodavatel nemůže Objednateli poskytnout oprávnění dle odst. 7.3 tohoto článku Smlouvy nebo to po něm nelze spravedlivě požadovat, je Dodavatel povinen zajistit, aby se jednalo o open source SW, který je veřejnosti poskytován zdarma (tato podmínka je splněna za předpokladu, že tento open source SW bude poskytován zdarma i Objednateli), včetně zdrojových kódů, úplné původní uživatelské, provozní a administrátorské dokumentace a práva takový SW měnit a současně je povinen zajistit, že právo Objednatele takový open source SW užít (např. licence) a způsob jeho použití nesmí kontaminovat zdrojový kód jakékoliv části Předmětu plnění dle Smlouvy, které jsou počítačovým programem, povinností jejich zveřejnění či povinnosti poskytnutí ostatních částí díla k volnému užití jakékoliv třetí straně.
	2. Udělení veškerých práv uvedených v tomto článku Smlouvy nelze ze strany Dodavatele vypovědět a na jejich udělení nemá vliv ukončení účinnosti této Smlouvy.
	3. Dodavatel prohlašuje, že veškeré jím dodané plnění podle této Smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní nebo jiný nárok plynoucí z právní vady poskytnutého Předmětu plnění dle této Smlouvy. V případě, že by nárok třetí osoby vzniklý v souvislosti s plněním Dodavatele dle této Smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání Předmětu plnění či jeho části, zavazuje se Dodavatel zajistit náhradní řešení a minimalizovat dopady takovéto situace, a to bez dopadu na cenu Předmětu plnění sjednanou dle této Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu škody.
	4. S nositeli chráněných práv duševního vlastnictví vzniklých v souvislosti s realizací Předmětu plnění dle této Smlouvy je Dodavatel povinen vždy smluvně zajistit možnost nakládání s těmito právy Objednatelem v rozsahu definovaném tímto článkem Smlouvy.
	5. Dodavatel podpisem této Smlouvy výslovně prohlašuje, že odměna za veškerá oprávnění poskytnutá Objednateli dle tohoto článku Smlouvy je již zahrnuta v Ceně dle čl. 5 odst. 5.2 této Smlouvy.
	6. Smluvní strany dále výslovně prohlašují, že pokud při poskytování Předmětu plnění dle této Smlouvy vznikne činností Dodavatele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, bude se mít za to, že je Objednatel oprávněn vykonávat majetková autorská práva k dílu spoluautorů tak, jako by byl jejich výlučným vykonavatelem a že Dodavatel udělil Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena dle čl. 5 odst. 5.2 této Smlouvy je

stanovena se zohledněním tohoto ustanovení a Dodavateli nevzniknou v případě vytvoření díla spoluautorů žádné nové nároky na odměnu.

* 1. Dodavatel je povinen Objednateli uhradit jakékoli majetkové a nemajetkové újmy, vzniklé v důsledku toho, že Objednatel nemohl Předmět plnění či jeho část dle této Smlouvy užívat řádně a nerušeně. Jestliže se jakékoliv prohlášení Dodavatele v tomto článku Smlouvy ukáže nepravdivým nebo Dodavatel poruší jinou povinnost dle tohoto článku Smlouvy, jde o podstatné porušení Smlouvy a Objednateli vzniká nárok na smluvní pokutu dle čl. 15 odst. 15.10 a/nebo 15.11 této Smlouvy.
	2. Bude-li Autorské dílo nebo jeho část dílem zaměstnaneckým (dle § 58 AZ) nebo dílem kolektivním (dle § 59 AZ), je Dodavatel povinen vypořádat práva s autory takových děl (zejména opatřit potřebné souhlasy autorů a uhradit veškeré odměny autorům) tak, aby práva k takovému Autorskému dílu Objednateli mohl poskytnout v plném rozsahu dle tohoto článku Smlouvy a jejích příloh. Předáním části Předmětu plnění, které je Autorským dílem, Dodavatel poskytuje Objednateli potřebné Licence SW k Autorskému dílu a zároveň tím stvrzuje, že veškerá práva s autory zaměstnaneckých či kolektivních děl řádně vypořádal a je oprávněn je poskytnout Objednateli.
	3. Smluvní strany prohlašují, že pokud nastanou pochybnosti o rozsahu práv Objednatele k Předmětu plnění, a to i kdykoliv budoucnu, budou všechna ustanovení této Smlouvy a jejích příloh vykládána s ohledem na účel této Smlouvy a vůli Smluvních stran poskytnout Objednateli takový Předmět plnění, u něhož není dán vendor lock-in, s kterým může Objednatel volně nakládat, zejména ho jakkoliv modifikovat, upravovat, měnit, zasahovat do něj, a to i prostřednictvím třetích osob, aniž by mu v tom bránily jakékoliv právní překážky nebo překážky neprávní (např. nedostatečná dokumentace či zdrojové kódy či nedostatek součinnosti Dodavatele).
	4. Je-li část plnění dle této Smlouvy chráněna jiným způsobem, než jako Autorské dílo (ochrana jiných práv k duševnímu vlastnictví), uplatní se ustanovení tohoto článku analogicky tak, aby byl splněn účel této Smlouvy, tj. aby Objednatel obdržel dílo vč. všech jeho součástí vč. možnosti jej užívat, poskytovat k užívání, udržovat a rozvíjet, a to tak, aby tak mohl činit i samostatně nebo prostřednictvím třetí osoby. Dodavatel je povinen k dosažení shora uvedeného účelu poskytnout rovněž související informace, zejm. zdrojové kódy, popisy databází, popisy architektury a jiné informace.
	5. Specifikace konkrétních poskytnutých oprávnění (Licencí SW) je uvedena v Příloze č. 5 této Smlouvy, v níž je blíže popsáno veškeré využití SW v rámci Předmětu plnění, jeho licenčních podmínky a další identifikace.
	6. Pro vyloučení všech pochybností se stanovuje, že licenční podmínky definované v tomto čl. 7 Smlouvy a Příloze č. 1 Smlouvy jsou nadřazené licenčním podmínkám předloženým Dodavatelem v rámci své Nabídky v Zadávacím řízení a tvořícím Přílohu č. 5 této Smlouvy.
	7. Pro vyloučení pochybností se stanoví, že časově neomezenou licencí je licence na maximální možnou dobu, po kterou je takovou licenci možno získat, zejm. na dobu trvání majetkových práv autora.

##### Vlastnické právo

* 1. V případě, že výsledkem činnosti Dodavatele v rámci plnění předmětu této Smlouvy nebude dílo chráněné předpisy o duševním vlastnictví, Objednatel nabude vlastnické právo k dané části Předmětu plnění okamžikem jeho převzetí, tj. okamžikem podpisu Akceptačního protokolu oběma Smluvními stranami.
	2. Dodavatel prohlašuje, že vlastnické právo a nebezpečí škody na věci ke všem hmotným součástem Předmětu plnění předaným Dodavatelem Objednateli v souvislosti s plněním předmětu Smlouvy přechází na Objednatele dnem jejich protokolárního předání Objednateli, tj. okamžikem podpisu Akceptačního protokolu oběma Smluvními stranami. Cena hmotných nosičů dat je již zahrnuta v ceně dle čl. 5 odst. 5.2 této Smlouvy.
	3. Nebezpečí škody na hmotném plnění vyplývajícím z této Smlouvy přechází na Objednatele okamžikem podpisu Akceptačního protokolu oběma Smluvními stranami.
	4. Smluvní strany pro vyloučení případných pochybností výslovně sjednávají, že vlastníkem veškerých dat, které Objednatel či jím pověřená třetí osoba vytvoří, je Objednatel.

##### Záruka za jakost, odpovědnost za vady

* 1. Dodavatel zaručuje, že Předmět plnění má vlastnosti a funkční specifikaci stanovené touto Smlouvou a že je způsobilý pro použití ke sjednanému účelu. Dodavatel Objednateli garantuje záruku za jakost vztahující se ke všem částem Předmětu plnění včetně jeho příslušenství pokrývá všechny jeho součásti, včetně produktů třetích stran, které byly využity při realizaci Předmětu plnění, a to po dobu dvaceti čtyř (24) měsíců ode dne podpisu Akceptačního protokolu oběma Smluvními stranami, tj. garantuje, že Předmět plnění si po tuto dobu zachová všechny takové vlastnosti, funkčnost a stanovenou účelovou způsobilost (dále jen „**záruka**“).
	2. Dodavatel poskytuje Objednateli záruku, že Předmět plnění (a každá jeho část) bude prost jakýchkoliv vad věcných, funkčních, právních i ostatních. Předmět plnění nebo jeho část má vady, jestliže zejména neodpovídá výsledku určenému ve Smlouvě, účelu jeho využití, případně nemá vlastnosti výslovně stanovené touto Smlouvou, Dokumentací, Objednatelem nebo právními předpisy. Záruka se vztahuje na vady, které se projeví během záruční doby s výjimkou vad, u nichž Dodavatel prokáže, že jejich vznik zapříčinil Objednatel.
	3. Veškeré složky Předmětu plnění musí být nové, nepoužité, nepoškozené a zhotovené z kvalitního materiálu. Veškeré složky Předmětu plnění musí být schopny podávat trvale standardní výkon v souladu s vlastnostmi a kvalitou stanovenou ve Smlouvě a plně vyhovovat účelu, pro který jsou jako součást Předmětu plnění dodávány. Hmotné a nehmotné věci tvořící součást Předmětu plnění nesmí být zatíženy právními vadami, např. zástavním právem.
	4. Uplatněním nároku z odpovědnosti za vady Předmětu plnění není dotčen nárok Objednatele na náhradu újmy. Smluvní strany se dohodly, že ustanovení § 1965, § 2103, § 2104, § 2111 a § 2112 občanského zákoníku se nepoužijí.
	5. Záruční doba se staví po dobu, po kterou nemůže Objednatel Předmět plnění a/nebo jeho část a/nebo jeho dílčí část řádně užívat pro vady, za které nese odpovědnost Dodavatel.
	6. Veškeré vady (reklamace) je Objednatel povinen uplatnit u Dodavatele bez zbytečného odkladu poté, kdy vadu zjistil, a to hlášením v souladu s odst. 9.11 tohoto článku Smlouvy, obsahujícím specifikaci zjištěné vady.
	7. Reklamaci lze uplatnit do posledního dne záruční doby, přičemž i reklamace odeslaná Objednatelem v poslední den záruční doby se považuje za včas uplatněnou.
	8. Dodavatel odpovídá za to, že Dokumentace a soubory dat, které Objednateli v rámci Předmětu plnění dle této Smlouvy předal:
		+ jsou autorizovanými kopiemi originálů příslušných dokumentů a souborů dat Dodavatele,
		+ neobsahují žádné infiltrační prostředky,
		+ že k nim má práva na jejich šíření, instalaci, konfiguraci a správu, která mu umožňují s nimi nakládat a dále je poskytovat tak, jak je sjednáno v této Smlouvě.
	9. V případě, že se některá z uvedených garancí Dodavatele ukáže nepravdivou a Objednateli z tohoto důvodu vznikne škoda, bude Dodavatel povinen Objednateli tuto škodu nahradit v celém rozsahu.
	10. Dodavatel uhradí škodu, která Objednateli vznikla vadným plněním v plné výši. Dodavatel rovněž Objednateli uhradí náklady vzniklé při uplatňování práv z odpovědnosti za vady.
	11. Vady budou zástupci Objednatele hlášeny Dodavateli prostřednictvím kontaktního místa pro hlášení vad:

Email: xxx

Telefon: xxx

* 1. Dodavatel je v souvislosti s řešením vad Předmětu plnění povinen zajistit provedení zásahů do provozního prostředí Objednatele dle pokynů Objednatele. Tyto zásahy nesmí mít dopad do provozu ostatních informačních systémů Objednatele, v opačném případě Dodavatel odpovídá za škodu Objednateli tím způsobenou.
	2. Vyplyne-li z objektivních skutečností potřeba delší reakční doby, než je prvotně určena Objednatelem, Objednatel je, prostřednictvím kontaktních osob uvedených v Příloze č. 4 této Smlouvy, oprávněn stanovit delší reakční dobu. Za objektivní skutečnosti lze považovat zejména zásah vyšší moci, chybnou funkci operačních a databázových platforem, časový rozsah potřebných prací jdoucí nad stanovený rámec.
	3. Pro účely Smlouvy je pro odstraňování vad v rámci záruky stanovena pracovní doba

v pracovních dnech od 8:00 do 16:00 hodin.

* 1. Smluvní strany pro vyloučení případných nejasností sjednávají, že záruka za jakost dle tohoto čl. 9 Smlouvy se nevztahuje na:
1. vady Předmětu plnění spočívající v nesouladu Předmětu plnění s právními předpisy, jež nabydou účinnosti po podpisu Akceptačního protokolu oběma Smluvními stranami,
2. vady GIS systému, k nimž došlo v příčinné souvislosti se změnami HW a SW Objednatele, nastavením a konfiguracemi HW a SW Objednatele provedenými Objednatelem, o nichž Dodavatel nebyl Objednatelem informován.

##### Obchodní tajemství, ochrana důvěrných informací

* 1. Smluvní strany sjednávají, že veškeré skutečnosti jakkoli se týkající nebo související se Smluvními stranami a veškeré další skutečnosti, o nichž se dozví v souvislosti s touto Smlouvou, jsou Smluvními stranami považovány za důvěrné, aniž by bylo nutné tyto informace jednotlivě jako důvěrné výslovně označovat (dále jen „**Důvěrné informace**“). Důvěrnými informacemi jsou zejména obsah veškerých dokumentů, dokladů a podkladů, které za účelem splnění závazků dle této Smlouvy zpřístupní Objednatel Dodavateli, a dále veškeré další informace, které za tímto účelem poskytne Objednatel Dodavateli v jakékoli podobě a jakoukoli formou.
	2. Smluvní strany se zavazují, že veškeré Důvěrné informace, které od sebe navzájem získají, budou použity výhradně pro účely řádného splnění závazků dle této Smlouvy a bude s nimi nakládáno jako s obchodním tajemstvím.
	3. Přijímající Smluvní strana se zavazuje používat k ochraně Důvěrné informace před jejím neoprávněným užíváním, poskytnutím, zveřejněním nebo šířením přiměřené péče, avšak v žádném případě ne v menší míře, než je míra péče, kterou využívá k ochraně svých důvěrných informací, které jsou podobného významu.
	4. Smluvní strany se zavazují, že Důvěrné informace jiným subjektům nesdělí, nezpřístupní, ani nevyužijí pro sebe nebo pro jinou osobu. Přijímající Smluvní strana může poskytnout či zpřístupnit jakoukoli Důvěrnou informaci třetí straně, která nebyla adresátem Důvěrné informace, pouze po obdržení písemného souhlasu sdělující Smluvní strany.
	5. Předávání Důvěrných informací bude probíhat dle volby Objednatele buď osobně formou protokolárního předání hmotných nosičů, na kterých budou Důvěrné informace zachyceny, nebo elektronickou formou. Důvěrné informace v elektronické podobě musí být bezpečně zašifrované při přenosu po datové síti nebo při uložení na datovém médiu. Použité kryptografické prostředky musí být v souladu s ustanovením § 26 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**VyKB**“).
	6. Každá ze Smluvních stran se zavazuje vynaložit maximální úsilí, aby tajnost Důvěrných informací druhé Smluvní strany byla důsledně dodržována jejími zaměstnanci i osobami, které v souladu s touto Smlouvou k plnění účelu spolupráce použije. Použije-li některá ze Smluvních stran k plnění třetí osoby, je oprávněna zpřístupnit jí Důvěrné informace získané od druhé Smluvní strany pouze v rozsahu nezbytně nutném pro jí poskytované plnění a je rovněž povinna zavázat třetí osobu povinností zachování Důvěrných informací v rozsahu dle této Smlouvy. Za porušení povinností třetí osobou odpovídá Smluvní strana, která jí Důvěrné informace zpřístupnila.
	7. Dodavatel zajistí, aby přístup k elektronickým datovým souborům obsahujícím osobní údaje a Důvěrné informace byl dostatečně zabezpečen v souladu s požadavky na důvěrnost a integritu dat podle VyKB.
	8. Je-li pro účel kontroly správného fungování GIS Systému nebo odstranění vady nezbytné poskytnout Dodavateli kopii databází, souborů nebo nosičů údajů obsahujících jakékoliv údaje z činnosti Objednatele a jím určených organizací, je Dodavatel povinen s takovými údaji nakládat tak, aby nedošlo k jejich úniku či zneužití.
	9. Veškeré skutečnosti obchodní, ekonomické a technické povahy související se Smluvními stranami, které nejsou běžně dostupné v obchodních kruzích a se kterými se Smluvní strany seznámí při realizaci předmětu Smlouvy nebo v souvislosti s touto Smlouvou, se považují za Důvěrné informace.
	10. Dodavatel se zavazuje, že Důvěrné informace jiným subjektům nesdělí, nezpřístupní, ani nevyužije pro sebe nebo pro jinou osobu, a nebude z nich pořizovat kopie ani opisy. Zavazuje se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo poddodavatelům, kteří jsou pověřeni plněním Smlouvy a za tímto účelem jsou oprávněni se s těmito informacemi v nezbytném rozsahu seznámit. Dodavatel

se zavazuje zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné

a zachovávaly o nich mlčenlivost.

* 1. Povinnost plnit ustanovení tohoto článku Smlouvy se nevztahuje na informace, které:
		+ je Smluvní strana povinna sdělit na základě zákonem stanovené povinnosti;
		+ byly písemným souhlasem poskytující Smluvní strany zproštěny těchto omezení;
		+ jsou známé nebo byly zveřejněny jinak, než následkem zanedbání povinnosti jedné ze Smluvních stran;
		+ příjemce je zná dříve, než je sdělí Smluvní strana;
		+ jsou vyžádány soudem, státním zastupitelstvím nebo příslušným správním orgánem na základě zákona;
		+ je Objednatel povinen poskytnout svému zakladateli;
		+ je Objednatel povinen poskytnout jakékoli třetí osobě.
	2. Povinnost ochrany Důvěrných informací trvá bez ohledu na ukončení účinnosti této Smlouvy.
	3. Smluvní strany se zavazují, že obchodní a technické informace, které jim byly svěřeny druhou stranou, nezpřístupní třetím osobám bez písemného souhlasu druhé strany a nepoužijí tyto informace k jiným účelům, než je k plnění podmínek této Smlouvy.
	4. Dodavatel je povinen nejpozději do čtrnácti (14) kalendářních dnů po ukončení účinnosti této Smlouvy jemu písemně předané Důvěrné informace, dle formy zachycení těchto písemných informací a dle dohody s Objednatelem Objednateli vrátit nebo je prokazatelně zničit. O vrácení či zničení dle tohoto odst. 11.14 Smlouvy musí být sepsán protokol, který musí být podepsán oprávněnými osobami obou Smluvních stran.

##### Nakládání s osobními údaji

* 1. Objednatel jako správce osobních údajů zpracovává osobní údaje Dodavatele, je-li Dodavatelem fyzická osoba, a obě Smluvní strany jako správci osobních údajů zpracovávají osobní údaje kontaktních osob poskytnuté ve Smlouvě, popřípadě osobní údaje dalších osob, které jsou poskytnuty v rámci Smlouvy, pouze a výhradně pro účely související s plněním Smlouvy, a to po dobu trvání této Smlouvy, resp. pro účely vyplývající z právních předpisů po dobu delší, která je těmito právními předpisy odůvodněna. Dodavatel je povinen informovat obdobně fyzické osoby, jejichž osobní údaje pro účely související s plněním Smlouvy Objednateli předává.
	2. Dodavatel nepředává Objednateli v rámci poskytnutí Předmětu plnění kromě případu uvedeného v odst. 11.1 tohoto článku Smlouvy žádné další osobní údaje. V případě,

že součástí Předmětu plnění bude předání osobních údajů podléhajících ochraně dle příslušných právních předpisů na ochranu osobních údajů, je Dodavatel povinen na tuto skutečnost Objednatele předem písemně upozornit a Objednatel je oprávněn dle svého uvážení převzetí osobních údajů odmítnout.

* 1. Pro případ, že Dodavatel v rámci plnění Smlouvy získá přístup k informacím, jež budou obsahovat osobní údaje podléhající ochraně dle právních předpisů, je Dodavatel oprávněn přistupovat k takovým osobním údajům pouze v rozsahu nezbytném pro plnění předmětu Smlouvy. Dodavatel se zavazuje nakládat se zpřístupněnými osobními údaji pouze na základě pokynů Objednatele, pouze pro účely plnění Smlouvy, zachovat o nich mlčenlivost a zajistit jejich bezpečnost proti úniku, náhodnému nebo neoprávněnému zničení, ztrátě, pozměňování nebo neoprávněnému zpřístupnění třetím osobám.
	2. Pokud řádné poskytování Předmětu plnění dle této Smlouvy vyžaduje zpracování osobních údajů zaměstnanců Objednatele, budou osobní údaje zaměstnanců Objednatele Dodavatelem zpracovány v následujícím rozsahu:
		1. jméno a příjmení,
		2. funkce / pozice,
		3. e-mail,
		4. telefonní číslo,
		5. osobní číslo.
	3. Zpracování osobních údajů je definováno příslušnou právní úpravou, přičemž se jedná zejména o jejich shromažďování, ukládání na nosiče informací, používání, třídění nebo kombinování, blokování a likvidace s využitím manuálních a automatizovaných prostředků v rozsahu nezbytném pro zajištění řádného poskytování Předmětu plnění dle této Smlouvy.
	4. Osobní údaje budou zpracovány po dobu poskytování Předmětu plnění dle této Smlouvy. Ukončením této Smlouvy nezanikají povinnosti Dodavatele týkající se bezpečnosti a ochrany osobních údajů až do okamžiku jejich protokolární úplné likvidace či protokolárního předání jinému zpracovateli.
	5. Smluvní strany se dohodly, že Dodavatel nemá nárok na náhradu nákladů spojených se zpracováním osobních údajů či s plněním povinností vyplývajících z příslušné právní úpravy.
	6. Objednatel je povinen přijmout vhodná opatření na to, aby poskytl subjektům údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace a učinil veškerá sdělení požadovaná Nařízením Evropského parlamentu a Rady (EU) č. 2016/679

ze dne 27. dubna 2016, obecného nařízení o ochraně osobních údajů (dále jen

„**Nařízení**“) ve spojení s právními předpisy upravujícími zpracování osobních údajů.

* 1. Dodavatel je při plnění této povinnosti povinen:
* nezapojit do zpracování osobních údajů žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení Objednatele;
* zpracovávat osobní údaje pouze na základě doložených pokynů Objednatele, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci;
* zohledňovat povahu zpracování osobních údajů a být Objednateli nápomocen pro splnění Objednatelovi povinnosti reagovat na žádosti o výkon práv subjektu údajů, jakož i pro splnění dalších povinností ve smyslu Nařízení;
* zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby, které budou mít přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby;
* zajistit, že jeho zaměstnanci budou zpracovávat osobní údaje pouze za podmínek a v rozsahu Dodavatelem stanoveném;
* na žádost Objednatele kdykoliv umožnit provedení auditu či inspekce týkající se zpracování osobních údajů;
* po skončení této Smlouvy protokolárně odevzdat Objednateli nebo nově pověřenému zpracovateli všechny osobní údaje zpracované po dobu poskytování Předmětu plnění.
	1. Smluvní strany jsou povinny:
* zavést technická, organizační, personální a jiná vhodná opatření ve smyslu Nařízení, aby zajistily a byly schopny kdykoliv doložit, že zpracování osobních údajů je prováděno v souladu s Nařízením a právními předpisy upravujícími zpracování osobních údajů tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům a k datovým nosičům, které tyto údaje obsahují, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití, a tato opatření podle potřeby průběžné revidovat a aktualizovat;
* vést a průběžné revidovat a aktualizovat záznamy o zpracování osobních údajů

ve smyslu Nařízení;

* řádně a včas ohlašovat případná porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a spolupracovat s tímto úřadem v nezbytném rozsahu;
* navzájem se informovat o všech okolnostech významných pro plnění dle tohoto článku Smlouvy např. změna sídla, právní formy, změna bankovního spojení, zrušení registrace k DPH;
* zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po skončení této Smlouvy;
* postupovat v souladu s dalšími požadavky Nařízení a právními předpisy upravujícími zpracování osobních údajů, zejména dodržovat obecné zásady zpracování osobních údajů, plnit své informační povinnosti, nepředávat osobní údaje třetím osobám bez potřebného oprávnění, respektovat práva subjektů údajů a poskytovat v této souvislosti nezbytnou součinnost.

##### Další práva a povinnosti Smluvních stran

* 1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si součinnost nezbytnou pro řádné provedení Předmětu plnění dle této Smlouvy. Smluvní strany jsou povinny informovat bezodkladně druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné provedení Předmětu plnění dle této Smlouvy. V případě prokazatelného prodlení povinné Smluvní strany s poskytnutím součinnosti není oprávněná Smluvní strana v prodlení s plněním svých závazků podle Smlouvy a veškeré lhůty se o prokazatelné prodlení povinné Smluvní strany prodlužují.
	2. Objednatel se zavazuje vyjadřovat se k návrhům na další postup, bude-li to nezbytné pro řádné dokončení Předmětu plnění a umožnit Dodavateli bezodkladně po uzavření Smlouvy přístup ke všem informacím a podkladům nezbytným pro realizaci Předmětu plnění, umožnit pracovníkům Dodavatele případný vstup do objektu Objednatele v pracovní dny. Za tímto účelem Dodavatel výslovně prohlašuje, že své pracovníky seznámil se zvláštními bezpečnostními a požárními opatřeními Objednatele a dále zvláštními předpisy platnými pro pracoviště Objednatele.
	3. Dodavatel se zavazuje při realizaci Předmětu plnění postupovat v profesionální kvalitě a s odbornou péčí.
	4. Osoby, které se na straně Dodavatele přímo a/nebo nepřímo podílejí na plnění dle této Smlouvy musí splňovat požadavky na personální bezpečnost danou platnou a účinnou legislativou v oblasti kybernetické bezpečnosti, zejména musí být řádně a prokazatelně proškoleni v oblasti bezpečnosti dat a informací, kvalifikovány k výkonu příslušných činností.
	5. Dodavatel se zavazuje dle této Smlouvy řádně a včas realizovat Předmět plnění,

a to v dohodnutém množství, jakosti a provedení.

* 1. Dodavatel je povinen při realizaci Předmětu plnění dodržovat veškeré bezpečnostní předpisy, veškeré zákony a jejich prováděcí vyhlášky, pokud se vztahují k prováděnému Předmětu plnění a týkají se činnosti Dodavatele, bezpečnosti práce, požární ochraně a ochraně životního prostředí. Pokud porušením těchto předpisů Dodavatelem vznikne škoda, nese náklady Dodavatel.
	2. Dodavatel se zavazuje, že nezpůsobí, resp. učiní vše nezbytné a vynaloží veškerou možnou péči, kterou lze po něm objektivně požadovat, aby nedošlo k narušení, poškození nebo zničení HW a SW Objednatele, narušení důvěrnosti dostupnosti a integrity dat Objednatele, a to včetně napadení systémů a dat Objednatele škodlivým SW, neoprávněným přístupem apod. Pokud i přes veškeré vynaložené úsilí Dodavatele dojde v důsledku zavinění Dodavatele k narušení, poškození nebo zničení HW a SW Objednatele, narušení důvěrnosti dostupnosti a integrity dat Objednatele ve smyslu předchozí věty, je Dodavatel povinen učinit vše nezbytné a vynaložit veškerou možnou péči, kterou lze po něm objektivně požadovat, aby takové porušení odstranil. To Dodavatele nezbavuje povinnosti uhradit Objednateli újmu vzniklou tímto porušením povinnosti ze strany Dodavatele.
	3. Dodavatel je povinen vyžádat si před jakýmkoli zásahem do GIS Systému, ke kterému dojde v průběhu trvání této Smlouvy (včetně update, legislativního update, upgrade, legislativního upgrade, mimořádného update a patche), předchozí prokazatelný souhlas oprávněné osoby Objednatele uvedené v Příloze č. 4 této Smlouvy nebo touto osobou pověřeného zástupce. Jakékoli zásahy do GIS Systému budou Dodavatelem prováděny vždy pod dohledem osoby, kterou Objednatel pro tyto účely určí.
	4. Dodavatel je povinen zajistit, že veškeré vlastnosti GIS Systému, včetně jeho update, legislativních update, upgrade a legislativních upgrade, mimořádných updatů a patchů budou po celou dobu účinnosti této Smlouvy odpovídat obecně závazným platným právním předpisům.
	5. Dodavatel Objednateli zaručuje, že v GIS Systému ani jakékoli jeho části není a nebude zabudován škodlivý kód (tzv. backdoor) umožňující neoprávněně a bez vědomí Objednatele zasahovat do GIS Systému na dálku a ovládat jej. V opačném případě Dodavatel odpovídá Objednateli za veškerou újmu vzniklou v souvislosti s porušením této povinnosti.
	6. Objednatel má právo přesvědčit se kdykoliv v průběhu plnění Předmětu plnění o stavu prací na Předmětu plnění včetně kontroly jakosti (náhled do zdrojového kódu vývojových prací, testování funkcionality) a Dodavatel mu k tomuto musí vytvořit podmínky. Případné náklady nese Dodavatel. Objednatel má zejména právo požadovat konání kontrolních schůzek v přiměřených termínech (s frekvencí 7 dnů, nedohodnou-li se pověřené osoby stran v konkrétních případech jinak). Objednatel si vyhrazuje právo účasti zástupců Koncového zákazníka (MV) nebo jeho poradce. Na

těchto schůzkách má Objednatel právo kontrolovat obsah plnění a klást dotazy a vznášet připomínky k obsahu plnění. Těmito připomínkami lze upřesňovat požadavky na plnění, nesmí však být provedena změna uzavřené smlouvy.

* 1. Dodavatel je povinen bez zbytečného odkladu písemně informovat Objednatele o skutečnostech, které mají nebo mohou mít vliv na plnění Smlouvy, a to neprodleně, nejpozději následující pracovní den poté, kdy příslušná skutečnost nastane nebo Dodavatel zjistí, že by nastat mohla.
	2. Zjistí-li Dodavatel při realizaci Předmětu plnění překážky bránící jeho řádnému provedení, je povinen to bez zbytečného odkladu písemně oznámit Objednateli a navrhnout mu další postup.
	3. Dodavatel je povinen účastnit se na základě písemné pozvánky Objednatele všech jednání týkajících se předmětu Smlouvy, řídit se při provádění plnění dle této Smlouvy jeho pokyny a poskytnout mu požadovanou Dokumentaci. Odměna za účast Dodavatele na jednáních dle tohoto odstavce Smlouvy, jakož i veškeré náklady Dodavatele spojené s účastí na těchto jednáních, jsou plně zahrnuty v Ceně dle čl. 5 odst. 5.2 této Smlouvy.
	4. Dodavatel je povinen řídit se ve smyslu ustanovení § 2592 občanského zákoníku příkazy Objednatele.
	5. Dodavatel se zavazuje nepoužít ve svých dokumentech jakýkoliv odkaz na název Objednatele nebo jakýkoliv jiný odkaz, který by mohl, byť i nepřímo, vést k identifikaci Objednatele, bez předchozího písemného souhlasu Objednatele.
	6. Dodavatel není oprávněn postoupit ani převést jakákoliv svá práva či povinnosti vyplývající ze Smlouvy bez předchozího písemného souhlasu Objednatele na třetí osoby. Dodavatel je oprávněn pověřit plněním závazků plynoucích ze Smlouvy jiné třetí osoby (poddodavatele), nebo takové třetí osoby (poddodavatele) změnit, uvedl-li je již ve své Nabídce, pouze s předchozím písemným souhlasem Objednatele. Pokud se jedná o takové třetí osoby (poddodavatele), kterými Dodavatel prokazoval kvalifikaci, tak musí tato nová třetí osoba (poddodavatel) splňovat kvalifikační předpoklady minimálně v rozsahu stanoveném v Zadávacím řízení. Pokud byla tato třetí osoba (poddodavatel) taktéž součástí hodnocení nabídek v Zadávacím řízení, tak musí taktéž splňovat kvalifikační předpoklady minimálně v takovém rozsahu, v jakém byly započteny do tohoto hodnocení nabídek v Zadávacím řízení u původní třetí osoby (poddodavatele). Dodavatel je povinen splnění náležitostí dle předchozí věty doložit před odsouhlasením této změny Objednatelem, a to stejnou formou, jaká byla vyžadována v Zadávacím řízení. Udělí-li Objednatel s využitím nebo změnou třetí osoby (poddodavatele) souhlas, je Dodavatel povinen zavázat poddodavatele k zachování Důvěrných informací a k ochraně osobních údajů ve smyslu čl. 10 a čl. 11 této Smlouvy ve stejném rozsahu, v jakém je k této povinnosti zavázán sám. Dodavatel

odpovídá za své poddodavatele jako za plnění vlastní, včetně odpovědnosti

za způsobenou újmu.

* 1. Jestliže vznikne na straně Dodavatele nemožnost plnění ve smyslu § 2006 občanského zákoníku, Dodavatel písemně uvědomí bez zbytečného odkladu o této skutečnosti a její příčině Objednatele. Pokud není jinak stanoveno písemně Objednatelem, bude Dodavatel pokračovat v realizaci svých závazků vyplývajících ze smluvního vztahu v rozsahu svých nejlepších možností a schopností a bude hledat alternativní prostředky pro realizaci té části plnění, kde není možné plnit. Pokud by podmínky nemožnosti plnění trvaly déle než třicet (30) kalendářních dnů, je Objednatel oprávněn od této Smlouvy odstoupit.
	2. Brání-li některé ze Smluvních stran v plnění povinností ze Smlouvy mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli ve smyslu ustanovení § 2913 odst. 2 občanského zákoníku, prodlužují se o dobu, po kterou trvá překážka, lhůty pro plnění povinností stanovených Smluvním stranám Smlouvou. Dodavatel je povinen o vzniku a zániku takové překážky Objednatele neprodleně informovat a tuto překážku Objednateli doložit. Jakmile překážka přestane působit, zavazuje se Dodavatel vyvinout maximální úsilí vedoucí k naplnění účelu Smlouvy a zavazuje se zajistit splnění povinností ze Smlouvy bez zbytečného odkladu.

##### Pojištění Dodavatele

* 1. Dodavatel se zavazuje mít po celou dobu účinnosti Smlouvy uzavřenou platnou a účinnou pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě s limitem pojistného plnění, který nesmí být nižší než 20 000 000,- Kč (slovy: dvacet milionů korun českých). V případě, že plněním této Smlouvy dojde ke způsobení škody Objednateli nebo třetím osobám, která nebude kryta pojištěním sjednaným ve smyslu tohoto odstavce Smlouvy, bude Dodavatel povinen tyto škody uhradit z vlastních prostředků.
	2. Dodavatel se zavazuje, po předchozí písemné žádosti Objednatele, předložit nejpozději do sedmi (7) kalendářních dnů k nahlédnutí Objednateli platnou a účinnou pojistnou smlouvu, a to i opakovaně. Bude-li zjištěno, že Dodavatel nedisponuje účinnou pojistnou smlouvou, jedná se o podstatné porušení Smlouvy a Objednatel je od této Smlouvy oprávněn odstoupit.

##### Vzájemná komunikace Smluvních stran a kontaktní osoby

* 1. Veškerá komunikace mezi Smluvními stranami je činěna písemně, není-li touto Smlouvou stanoveno jinak, a to v listinné nebo elektronické podobě prostřednictvím doporučené pošty, e-mailu či datové schránky. Pro operativní komunikaci je možné

využít též telefonického nebo osobního kontaktu, nicméně následně musí dojít

k potvrzení ústního ujednání písemnou formou.

* 1. Veškerá oznámení mezi Smluvními stranami, která se vztahují ke Smlouvě, nebo která mají být učiněna na základě Smlouvy a která mají či mohou mít jakýkoliv účinek na trvání, změnu či ukončení této Smlouvy, musí být učiněna v písemné podobě a druhé Smluvní straně doručena buď osobně nebo doporučeným dopisem či jinou formou registrovaného poštovního styku na adresu uvedenou v záhlaví této Smlouvy, není-li Smlouvou stanoveno nebo mezi Smluvními stranami pro konkrétní případy písemně dohodnuto jinak.
	2. Veškerou koordinaci případných poddodavatelů Dodavatele zajišťuje Dodavatel, nikoli Objednatel. Pokud si Objednatel nevyžádá jinak, bude komunikace vedena pouze na úrovni Objednatel – Dodavatel, nikoli mezi Objednatelem a případnými jednotlivými poddodavateli.
	3. Smluvní strany se zavazují, že v případě změny své adresy budou o této změně druhou Smluvní stranu prokazatelně písemně informovat nejpozději do pěti (5) pracovních dnů.
	4. Kontaktní osoby Objednatele a Dodavatele pro účely této Smlouvy jsou uvedeny v Příloze č. 4 této Smlouvy. Smluvní strany pro vyloučení případných nejasností sjednávají, že kontaktní osoby Dodavatele a Objednatele v oblasti GIS Systému jsou oprávněny zejména předávat a přebírat Předmět plnění této Smlouvy, tj. podepisovat Akceptační protokol a vznášet požadavky a připomínky v rámci realizace Předmětu plnění.
	5. Obě Smluvní strany jsou oprávněny jednostranně změnit kontaktní osoby uvedené v Příloze č. 4 této Smlouvy bez nutnosti uzavření dodatku ke Smlouvě, přičemž změna je účinná doručením písemného oznámení o takové změně druhé Smluvní straně.

##### Odpovědnost za škodu a sankční ujednání

* 1. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a této Smlouvy. Každá ze Smluvních stran nese odpovědnost za škodu způsobenou při plnění závazků ze Smlouvy v důsledku porušení povinností vyplývajících z obecně závazných právních předpisů či vyplývajících ze Smlouvy. Obě Smluvní strany se zavazují vyvíjet maximální úsilí k předcházení škodám a k minimalizaci vzniklých škod.
	2. Dodavatel odpovídá za škodu, kterou způsobil Objednateli v souvislosti s plněním Smlouvy nedodržením nebo porušením svých povinností vyplývajících ze Smlouvy. Odpovědnost za škodu způsobenou porušením smluvní povinnosti se řídí ustanovením

§ 2913 a násl. občanského zákoníku. Dodavatel se zároveň zavazuje Objednatele

odškodnit za jakékoliv škody, které Objednateli v důsledku porušení povinností Dodavatele vzniknou na základě pravomocného rozhodnutí soudu či jiného státního orgánu.

* 1. Žádná ze Smluvních stran není povinna nahradit škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. V případě, že Objednatel poskytl Dodavateli chybné zadání a Dodavatel s ohledem na svou povinnost provést Předmět plnění či jeho část s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.
	2. Žádná ze Smluvních stran není odpovědná za škodu vzniklou porušením povinnosti z této Smlouvy, prokáže-li, že mu ve splnění povinnosti ze Smlouvy dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli. Překážka vzniklá ze škůdcových osobních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním povinnosti ze Smlouvy v prodlení, ani překážka, kterou byl škůdce podle Smlouvy povinen překonat, ho však povinnosti k náhradě nezprostí. Smluvní strany se zavazují upozornit druhou stranu bez zbytečného odkladu na vzniklé překážky bránící řádnému plnění Smlouvy a dále se zavazují k vyvinutí maximálnímu úsilí k jejich odvrácení a překonání.
	3. Výše náhrady škody či jiné újmy se řídí občanským zákoníkem a její maximální výše není omezena. Dodavatel bere na vědomí, že výše škody, kterou může Objednateli způsobit, není omezena výší pojistky a zároveň Dodavatel rovněž prohlašuje, že je mu znám přibližný objem finančních prostředků, s nimiž Objednatel hospodaří.
	4. Škoda se hradí v penězích, nebo, je-li to možné nebo účelné, uvedením do předešlého stavu podle volby poškozené strany v konkrétním případě.
	5. V případě, že činností Dodavatele dojde ke způsobení škody Objednateli nebo třetím osobám, která nebude kryta pojištěním odpovědnosti dle čl. 13 této Smlouvy, bude Dodavatel povinen škodu uhradit z vlastních prostředků.
	6. V případě porušení prohlášení Dodavatele dle čl. 1 odst. 1.2 této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých) za každé jednotlivé porušení.
	7. V případě prodlení Dodavatele s poskytnutím Předmětu plnění dle Smlouvy je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 25 000,- Kč (slovy: dvacet pět tisíc korun českých), a to za každý i započatý kalendářní den prodlení.
	8. V případě, že se jakékoliv prohlášení Dodavatele v čl. 7 této Smlouvy ukáže nepravdivým nebo Dodavatel poruší jinou povinnost dle tohoto článku Smlouvy, je

Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 1 000 000 Kč (slovy: jeden milion korun českých) za každé jednotlivé porušení povinnosti.

* 1. V případě prodlení Dodavatele s předáním zdrojového kódu nebo jeho změny ve smyslu čl. 7 odst. 7.4 a 7.5 této Smlouvy a/nebo v případě neprokázání skutečnosti dle čl. 7 odst. 7.6 písm. a) této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši ve výši 5 000 Kč (slovy: pět tisíc korun českých), a to za každý i započatý kalendářní den prodlení.
	2. V každém jednotlivém případě porušení závazku Dodavatele k ochraně Důvěrných informací dle čl. 10 této Smlouvy je Objednatel oprávněn požadovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých).
	3. V každém jednotlivém případě porušení povinnosti Dodavatele při nakládání s osobními údaji dle čl. 11 této Smlouvy je Objednatel oprávněn požadovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých).
	4. V případě každého jednotlivého porušení povinnosti Dodavatele dle čl. 12 této Smlouvy je Objednatel oprávněn požadovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 50 000,- Kč (slovy: padesát tisíc korun českých).
	5. V případě porušení povinností Dodavatele plynoucích z čl. 13 této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 100 000,- Kč (slovy: jedno sto tisíc korun českých) za každé jednotlivé porušení.
	6. V případě nedodržení či porušení povinností Dodavatele vyplývajících ze ZoKB a VyKB a uvedených v čl. 16 této Smlouvy, je Objednatel oprávněn vyúčtovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých) za každý jednotlivý případ porušení těchto povinností.
	7. V případě nedodržení lhůty splatnosti faktury, kterou od Dodavatele převzal Objednatel k úhradě, se Objednatel zavazuje Dodavateli uhradit zákonný úrok z prodlení dle nařízení vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob, v platném znění.
	8. Vyúčtování smluvní pokuty / úroků z prodlení – penalizační faktura, musí být druhé Smluvní straně zasláno doporučeně s dodejkou. Smluvní pokuta je splatná ve lhůtě třiceti (30) kalendářních dnů ode dne doručení penalizační faktury. Úhrada smluvní pokuty / úroků z prodlení se provádí bankovním převodem na účet oprávněné Smluvní

strany uvedený v penalizační faktuře. Částka se považuje za zaplacenou okamžikem jejího připsání ve prospěch účtu oprávněné Smluvní strany.

* 1. Uplatněním jakékoliv smluvní pokuty není nijak dotčeno právo Objednatele na náhradu vzniklé újmy v celém rozsahu způsobené újmy.
	2. Objednatel je v případě uplatnění smluvní pokuty vůči Dodavateli dle této Smlouvy v případě neuhrazení smluvní pokuty ze strany Dodavatele oprávněn využít institut započtení vzájemných pohledávek.

##### Kybernetická bezpečnost

* 1. Správcem budovaného informačního systému v rámci projektu „Vybudování Informačního systému pro veřejné služby a služby veřejné správy INSPIRE“ je Ministerstvo vnitra České republiky, Nad Štolou 936/3, 170 34 Praha 7 (MV). Správce informačního systému stanovil, že vytvořený informační systém musí splňovat bezpečnostní požadavky shodně, jako na významný informační systém (dále jen „**VIS**“) dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „**ZoKB**“). Důvodem je, že informační systém bude po vybudování naplňovat určující kritéria pro VIS.
	2. Dodavatel podpisem této Smlouvy akceptuje, že dodávané plnění dle této Smlouvy je ve prospěch informačního systému, na který jsou kladeny bezpečnostní požadavky stejné jako na významný informační systém (VIS) dle ZoKB, a současně se zavazuje k zavedení a dodržování veškerých souvisejících bezpečnostních opatření požadovaných ZoKB a VyKB, a to minimálně po dobu plnění dle této Smlouvy.
	3. Dodavatel je povinen:
		1. umožnit Objednateli provedení zákaznického auditu u Dodavatele a poskytnout mu k němu nezbytnou součinnost (dále jen „**zákaznický audit**“). Objednatel je oprávněn provést zákaznický audit v případě auditu kybernetické bezpečnosti, dle

§ 16 VyKB Objednatelem provozovaného VIS. Dále lze provést zákaznický audit v případě řešení kybernetického bezpečnostního incidentu v přímé souvislosti s plněním dle této Smlouvy. Zákaznický audit může za Objednatele provést pověřený zaměstnanec Objednatele nebo jiná pověřená osoba. Objednatel je oprávněn pověřit provedením zákaznického auditu třetí stranu. Rozsah auditu musí být rozsahem relevantní k předmětu a účelu této Smlouvy;

* + 1. dodržovat při poskytování Předmětu plnění příslušná ustanovení bezpečnostních politik, metodik a postupů předaných Dodavateli Objednatelem, resp. platné řídící dokumentace Objednatele či její části anebo platné řídící dokumentace, k jejímuž dodržování se Objednatel zavázal, pokud byl Dodavatel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl s takovou

dokumentací Objednatele seznámen (např. školením, protokolárním předáním příslušné dokumentace Dodavateli, elektronickým předáním prostřednictvím e- mailu, zřízením přístupu Dodavateli na sdílené úložiště aj.). V případě provedených změn v bezpečnostní dokumentaci VIS, bude Dodavatel informován. Dodavatel je povinen řídit se novým obsahem bezpečnostní dokumentace VIS od data stanoveného Objednatelem, nejdříve však ode dne, kdy byl o změně informován;

* + 1. informovat neprodleně Objednatele o kybernetických bezpečnostních incidentech na straně Dodavatele souvisejících s plněním dle této Smlouvy, a které by mohly mít dopad na kybernetickou bezpečnost u Objednatele. Kybernetický bezpečnostní incident je definován ustanovením § 7 odst. 2 ZoKB;
		2. informovat neprodleně Objednatele o změně ovládání Dodavatele podle zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích) nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s aktivy určených k plnění dle této Smlouvy.
	1. Dodavatel je při poskytování Předmětu plnění pro Objednatele oprávněn užívat data předaná Dodavateli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
	2. Dodavatel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy, zejména ZoKB, VyKB a dalšími souvisejícími právními předpisy.
	3. Dodavatel bere na vědomí, že přístup k datům, informacím či zařízením souvisejícím s předmětem Smlouvy je možné povolit pouze fyzické identitě zaměstnance Dodavatele nebo poddodavatele Dodavatele zaevidované, a to na základě požadavku Dodavatele na přístup.
	4. Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno zásadou tzv. „potřeba vědět“ (need to know) a není nárokové.
	5. Dodavatel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Dodavatele nebo poddodavatele Dodavatele.
	6. Dodavatel se zavazuje, že nebude instalovat a používat žádné nástroje, které nebyly předem písemně odsouhlaseny Objednatelem a jejichž užívání by mohlo ohrozit kybernetickou bezpečnost.
	7. Dodavatel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části technologického nebo komunikačního systému programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci technologického nebo komunikačního systému nebo nelegální získání dat a informací. Dodavatel bere na vědomí, že přístup do interní sítě a/nebo k technologickým a komunikačním systémům bude realizován

s využitím zařízení Objednatele. V případě, že Objednatel povolí Dodavateli přístup do interní sítě a/nebo k technologickým a komunikačním systémům Objednatele ze zařízení Dodavatele, musí veškerá tato zařízení Dodavatele splňovat příslušné bezpečnostní standardy Objednatele.

* 1. Dodavatel se během poskytování Předmětu plnění pro Objednatele zavazuje dostatečně zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost.
	2. Dodavatel se zavazuje plnit požadavky Objednatele v oblasti likvidace dat (ať už dat na papírových médiích, dat zpracovávaných elektronicky nebo prostřednictvím jakýchkoliv dalších nosičů dat) dle přílohy č. 4 VyKB.
	3. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování Předmětu plnění Objednateli, kteří přistupují do interní sítě a/nebo technologického nebo komunikačního systému chránili autentizační prostředky a údaje k systémům Objednatele. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako bezpečnostní incident ve smyslu příslušné řídící dokumentace a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu platí pro Dodavatele, pokud byl s takovou řídící dokumentací Objednatele seznámen).
	4. Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či skutečnost vzniklá v důsledku porušení bezpečnostních požadavků nebude posuzována jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Dodavateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Dodavatele za prodlení obsažená v Smlouvě nejsou tímto ustanovením dotčena.
	5. Dodavatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost ke splnění povinností Objednatele zejména při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.
	6. Dodavatel se zavazuje dodržovat požadavky Objednatele na řízení kontinuity činností.
	7. Dodavatel stanoví činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních událostí a incidentů, podle takto stanovených a popsaných pravidel bude postupovat, a bude hlásit všechny bezpečnostní události a incidenty neprodleně po jejich detekci Objednateli prostřednictvím ohlašovacích kanálů Objednatele, v případech, kdy situace nestrpí odklad telefonicky. Dále se zavazuje vyhodnotit informace o bezpečnostních událostech a incidentech a o těchto informacích, vzniklých bezpečnostních incidentech, vč. krátkodobých a dlouhodobých

nápravných opatřeních nad všemi částmi řešení, které jsou ve správě Dodavatele, a rizicích souvisejících s ohrožením kontinuity činností vést přiměřené záznamy a tyto uchovat pro jejich budoucí použití s ohledem na požadavky Objednatele a legislativy České republiky. Nastavená pravidla a postupy podléhají schválení Objednatelem.

* 1. Dodavatel provede analýzu příčin bezpečnostního incidentu a navrhne opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

##### Doba trvání Smlouvy, ukončení Smlouvy

* 1. Tato Smlouva nabývá platnosti dnem podpisu oběma Smluvními stranami a účinnosti uveřejněním v registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, a uzavírá se na dobu neurčitou.
	2. Tuto Smlouvu lze předčasně ukončit:
		1. písemnou dohodou Smluvních stran, nebo
		2. jednostranným odstoupením z důvodů stanovených právními předpisy nebo touto Smlouvou, nebo v případě podstatného porušení Smlouvy.
	3. Za podstatné porušení smluvních povinnosti Dodavatele, za kterých může Objednatel od této Smlouvy odstoupit, se považuje zejména:
		1. prodlení Dodavatele s předáním Předmětu plnění dle Smlouvy Objednateli delší než třicet (30) kalendářních dní;
		2. opakované, tj. nejméně 2x během šedesáti (60) po sobě jdoucích kalendářních dnů, nesplnění pokynu Objednatele při realizaci Předmětu plnění Dodavatelem, a/nebo bránění Objednateli v provádění kontrol a testů Předmětu plnění nebo jeho části;
		3. opakované, tj. nejméně 2x během šedesáti (60) po sobě jdoucích kalendářních dnů, nebo hrubé porušení pravidel bezpečnosti práce, protipožární ochrany, ochrany zdraví při práci či jiných bezpečnostních předpisů a pravidel Dodavatelem nebo jeho poddodavatelem v místě plnění;
		4. porušení ochrany obchodního tajemství, ochrany Důvěrných informací a/nebo ochrany osobních údajů;
		5. porušení povinnosti poskytnutí Licencí SW v rozsahu dle této Smlouvy;
		6. Dodavatel předá Předmět plnění nebo jeho část, Dokumentaci, a/nebo jakékoli informace o prováděných činnostech třetí osobě (nevyplývá-li z příslušných ustanovení této Smlouvy, že tak Dodavatel učinit může), nebo jinak poruší své závazky dle této Smlouvy.
	4. Objednatel je rovněž oprávněn odstoupit od Smlouvy v případě blíže popsaném v čl. 3 odst. 3.1 této Smlouvy.
	5. Objednatel je rovněž oprávněn odstoupit od Smlouvy je-li Dodavatel v likvidaci nebo vůči jeho majetku probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh byl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek byl zcela nepostačující nebo byla zavedena nucená správa podle zvláštních právních předpisů.
	6. Za podstatné porušení smluvních povinností Objednatelem, za kterých může Dodavatel od této Smlouvy odstoupit, se považuje prodlení Objednatele s úhradou faktury delší než šedesát (60) kalendářních dní.
	7. Odstupuje-li od Smlouvy kterákoliv ze Smluvních stran, oznámí písemně tuto skutečnost druhé Smluvní straně, a to nejpozději do deseti (10) kalendářních dnů ode dne, kdy se tato Smluvní strana o důvodech zakládajících možnost odstoupení od této Smlouvy dozvěděla. Odstoupení je účinné doručením písemného oznámení o odstoupení druhé Smluvní straně.
	8. Odstoupení od této Smlouvy ze strany Objednatele není spojeno s uložením jakékoliv sankce k tíži Objednatele.
	9. Odstupuje-li některá ze Smluvních stran od této Smlouvy po podpisu Akceptačního protokolu oběma Smluvními stranami, zaniká Smlouva s účinky ex nunc.
	10. Při zániku závazku odstoupením jedné ze Smluvních stran s účinky ex nunc má Dodavatel právo na úplatu za plnění, které bylo řádně a bez vad (ve vztahu k povaze tohoto plnění) poskytnuto před účinností odstoupení. Objednateli v takovém případě náleží poskytnuté plnění.
	11. Plnění řádně poskytnutá ke dni ukončení Smlouvy dohodou si Smluvní strany nebudou vracet, nebude-li v konkrétním případě Smluvními stranami dohodnuto jinak. V případě sjednání vracení plnění jsou Smluvní strany povinny vzájemnou dohodou písemně vypořádat dosavadní přijaté smluvní plnění nejpozději do šedesáti (60) kalendářních dnů od zániku této Smlouvy.
	12. Ukončením účinnosti Smlouvy nebo její části nejsou dotčena ustanovení týkající se smluvní pokuty, záruky, náhrady újmy a jiných nároků a jiné přetrvávající závazky.

##### Závěrečná ustanovení

* 1. Právní vztahy výslovně Smlouvou neupravené se řídí relevantními ustanoveními občanského zákoníku.
	2. Smluvní strany prohlašují, že jsou si vědomi skutečnosti, že tato Smlouva bude uveřejněna v registru smluv v souladu se zákonem č. 340/2015 Sb., o registru smluv. Uveřejnění Smlouvy v registru smluv zajistí Objednatel.
	3. Dodavatel prohlašuje a potvrzuje, že na sebe přebírá nebezpečí změny okolností

ve smyslu ustanovení § 1765 odst. 2 občanského zákoníku.

* 1. Smluvní strany si ve smyslu ustanovení § 1794 odst. 2 občanského zákoníku ujednaly, že se Dodavatel výslovně vzdává jeho práva ve smyslu ustanovení § 1793 občanského zákoníku a souhlasí s cenou tak, jak byla Smluvními stranami sjednána výše v této Smlouvě.
	2. Všechny spory, které vzniknou ze Smlouvy nebo v souvislosti s ní a které se nepodaří vyřešit přednostně smírnou cestou, budou rozhodovány obecnými soudy v souladu s ustanoveními zákona č. 99/1963 Sb., občanského soudního řádu, ve znění pozdějších předpisů. Místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.
	3. Pokud jakákoliv ustanovení nebo jakékoliv části ustanovení Smlouvy budou považovány za neplatné nebo nevymahatelné, nebude mít taková neplatnost nebo nevymahatelnost za následek neplatnost nebo nevymahatelnost celé Smlouvy, ale celá Smlouva se bude vykládat tak, jako kdyby neobsahovala příslušná neplatná nebo nevymahatelná ustanovení nebo části ustanovení a práva a povinnosti Smluvních stran se budou vykládat přiměřeně. Smluvní strany se dále zavazují, že budou navzájem spolupracovat s cílem nahradit takové neplatné nebo nevymahatelné ustanovení platným a vymahatelným ustanovením, jímž bude dosaženo stejného ekonomického výsledku (v maximálním možném rozsahu v souladu s právními předpisy), jako bylo zamýšleno ustanovením, jež bylo shledáno neplatným či nevymahatelným.
	4. Dnem doručení písemností odeslaných na základě této Smlouvy nebo v souvislosti s touto Smlouvou prostřednictvím provozovatele poštovních služeb, pokud není prokázán jiný den doručení, se rozumí poslední den lhůty, ve které byla písemnost pro adresáta uložena u provozovatele poštovních služeb, a to i tehdy, jestliže se adresát o jejím uložení nedověděl. Smluvní strany tímto výslovně vylučují ustanovení

§ 573 občanského zákoníku.

* 1. Smlouva může být měněna pouze dohodou Smluvních stran v písemné formě, přičemž změna Smlouvy bude účinná k okamžiku stanovenému v takovéto dohodě. Nebude-li takovýto okamžik stanoven, pak změna Smlouvy bude účinná ke dni uzavření takovéto dohody. Podstatná změna textu této Smlouvy nebo změna, která by nebyla připuštěna zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, je vyloučena.
	2. Tato Smlouva je vyhotovena elektronicky a podepsána oběma zástupci Smluvních stran zaručeným elektronickým podpisem.
	3. Nedílnou součástí Smlouvy jsou následující přílohy:

Příloha č. 1 – Technická specifikace Předmětu plnění Příloha č. 2 – Položkový rozpad ceny Předmětu plnění Příloha č. 3 – Vzory Akceptačního protokolu

Příloha č. 4 – Kontaktní osoby Smluvních stran Příloha č. 5 – Licenční podmínky

Příloha č. 6 – Rámcová pravidla vývoje aplikací pro ISSI

* 1. Smluvní strany prohlašují, že tato Smlouva je projevem jejich pravé a svobodné vůle a nebyla sjednána v tísni ani za jinak jednostranně nevýhodných podmínek. Na důkaz toho připojují Smluvní strany své podpisy.

|  |  |
| --- | --- |
| V Praze dne:  | V Praze dne:  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
| xxx |  | xxx |
| xxx**Národní agentura pro komunikační a informační technologie, s. p.** |  | xxx**SEVITECH CZ s.r.o.** |

#### Příloha č. 1 – Technická specifikace Předmětu plnění

*samostatný soubor - 693 stran*

#### Příloha č. 2 – Položkový rozpad ceny Předmětu plnění









**Příloha č. 3 – Vzor Akceptačního protokolu**

**AKCEPTAČNÍ PROTOKOL Č.**

|  |  |
| --- | --- |
| Objednatel | *Národní agentura pro komunikační a informační technologie, s. p.* |
| Dodavatel | *Název Dodavatele, adresa (dle Smlouvy)* |
| Smlouva | *Označení Smlouvy* |
| Název Projektu | *Označení Projektu* |
| Číslo Projektu | *Číslo Projektu* |

### Předmět akceptace

Předmětem akceptace je část Předmětu plnění uvedená v následující tabulce:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Číslo | Popis | Akceptováno | Akceptováno s výhradou | Neakceptováno |
| 01 | Popis předmětu Akceptace | X |  |  |
| 02 | Popis předmětu Akceptace | X |  |  |

### Výhrady

Seznam výhrad je uveden v následující tabulce:

|  |  |  |  |
| --- | --- | --- | --- |
| Číslo | Popis výhrady | Kategorie vady | Termín pro vypořádání vady |
| 01 | Popis výhrady Akceptace (popis výhrad lze nahradit odkazem na přílohu) |  |  |
| 02 | Popis výhrady Akceptace |  |  |

### Seznam příloh

Předávací protokoly jednotlivých částí Seznam předané dokumentace

Ostatní dokumenty nutné pro akceptaci dle Smlouvy s Dodavatelem

### Závěrečná ustanovení

Národní agentura pro komunikační a informační technologie, s. p. a Dodavatel svým podpisem stvrzují akceptaci části Předmětu plnění dle Smlouvy.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Jméno a příjmení | Datum | Podpis |
| Akceptoval za Objednatele |  |  |  |
| Akceptoval za Dodavatele |  |  |  |

#### Příloha č. 4 – Kontaktní osoby Smluvních stran

Za Objednatele:

* ve věcech smluvních a obchodních:

xxx

* ve věcech technických:

xxx

Za Dodavatele:

* ve věcech smluvních a obchodních: xxx
* ve věcech technických:

xxx

#### Příloha č. 5 – Licenční podmínky

##### Přehled použitého proprietárního software

Pro vytvoření navrhované platformy bude použit proprietární software **hale»connect**. Tím se výrazně sníží celkové náklady oproti vývoji nového řešení a také se zkrátí doba od zahájení projektu do produkce. Navíc budou sníženy náklady na údržbu oproti novému řešení, protože úsilí potřebné pro mnohé ze změn, jakými jsou např. změny Technické návody pro INSPIRE („INSPIRE Technical Guidance“) je „rozmělněno“ mezi velký počet zákazníků.

##### Licenční podmínky SW

hale»studio: opensource poskytovaný pod licenciou LGPL 3.0 33 INSPIRE Validator (ETF WebApp 2.0.0+): Open Source, EUPL 1.234 Grafana: Open Source, AGPL 3.035

Prometheus: Open Source, AGPL 3.036

PostgreSQL / PostGIS: Open Source, GNU GPL 2.037 hale»connect: proprietární

Do řešení je zahrnutá jedna specifická licenci na hale»connect, která může být použita:

* Počet organizací: až do počtu 5
* Počet jmenovaných uživatelů: až do počtu 25
* Maximální počet testovacích / výv. deploymentů: 10
* Maximální počet produkčních deploymentů: 3

hale»connect se sice neposkytuje jako opensource, ale licence poskytovaná v rámci tohoto projektu obsahuje tato ustanovení o přístupnosti zdrojového kódu:

Klient smí kdykoli požádat o kontrolu („inspect“) zdrojového kódu jakékoli části aplikace. Klient smí také požádat o přístup ke zdrojovému kódu pro účely auditů třetí stranou.

Klient dále smí požádat o kopii zdrojového kódu pro provedení vlastních změn na code base. Tyto změny mohou být provedeny pouze pro systém, pro který byla udělena původní licence. V takovém případě dodavatel pak již nenese odpovědnost za žádné problémy způsobené používáním softwaru.

Pokud by dodavatel kdykoli přestal software nabízet a udržovat, klient obdrží přístup k úplné kopii zdrojového kódu poslední verze, na kterou byla klientovi udělena licence (escrow zdrojového kódu). V takovém případě klient získá právo zdrojový kód upravit a nevýhradní právo distribuovat jej v jakékoli formě.

<https://www.gnu.org/licenses/lgpl-3.0.html> <https://joinup.ec.europa.eu/collection/eupl/eupl-text-eupl-12> <https://www.gnu.org/licenses/agpl-3.0.en.html> <https://www.gnu.org/licenses/agpl-3.0.en.html> <https://www.gnu.org/licenses/old-licenses/gpl-2.0.html>

*samostatný soubor - 30 stran*

**Příloha č. 6 – Rámcová pravidla vývoje, dodávek a souvisejících procesů a postupů**

**pro Informační systém pro veřejné služby a služby veřejné správy INSPIRE (ISSI)**

1. **Úvod**

Dokument nastavuje pravidla pro vývoj aplikací, webových portálů, SW řešení a formu spolupráce v prostředí Azure DevOps a návazné procesy vývoje včetně bezpečného vývoje pro projekt ISSI.

Na jednotlivé části plnění se užijí pouze ty číslované kapitoly těchto pravidel, které jsou pro příslušnou část plnění relevantní.

##### Cílem je:

* + Standardizace a popis procesu a nutných předpokladů k předání binárních artefaktů a zdrojových kódů.
	+ Odsouhlasení si jednotlivých kroků. Standardizace životního cyklu zdrojového kódu a přiřazení odpovědností.
	+ Stanovení politiky verzování, jak pro zdrojové kódy, tak i binární artefakty (verzování jednotlivých dodávek jako celku).
	+ Formální (závazný) popis požadavků implementace „automatizace“, tzn. politik GITu, kompilátorů a Cl/CD pipeline způsobem, že vynucení „bezpečného vývoje“ bude implicitní.
	+ Základní identifikace procesu modelování hrozeb na úrovni komponent aplikace.
	+ Pravidla pro externí programátory a vymezení základních pravidel, která budou v souladu s metodikou.
	+ Navazuje na systém řízení bezpečnosti informací Ministerstva vnitra (dále jen „**ISMS MV**“) a detailněji rozpracovává bezpečnostní požadavky stanovené bezpečnostními politikami ISMS MV v souvislosti s vývojem aplikací pro projekty. S tím, že tyto aplikace jsou určeny, nebo naplňují určovací kritéria, jako kritická informační infrastruktura nebo významný informační systém dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZoKB**“), a musí splňovat bezpečnostní požadavky určené legislativou v oblasti kybernetické bezpečnosti, především vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen

„**VyKB**“).

Vývojový tým (DEV tým) je tým vývojářů NAKIT a subdodavatele. Provozní tým (OPS tým) NAKIT, může využít služeb subdodavatelů na konkrétní úkoly na základě smluvního vztahu.

##### Technické požadavky

* + Vývojové prostředí DEV NAKIT slouží pro potřeby vývoje a skládá se z AKS (Azure Kubernetes service) a dalších podpůrných serverů jako SQL servery, Redis, Azure Search, Azure Cosmos DB, Azure KeyVault apod. Členům OPS týmu budou předávány funkční SW celky. DEV NAKIT je oficiálním prostředím, které je ekvivalentem k TEST NAKIT. Prostředí samotných vývojářů mimo NAKIT je považováno za nedůvěryhodné pro jakékoliv reklamace, nebo srovnávání funkcionalit a provozu systému.
	+ NAKIT GIT prostředí je chápáno jako primární. NAKIT může upravovat zdrojové kódy na základě autorských a licenční práv. Programátoři partnerů jsou zodpovědní za správný kontinuální přenos zdrojových kódů do určených repositářů. Pro hladký vývoj doporučujeme využívat pouze NAKIT GIT prostředí v Azure DevOps s jednotným GIT policy a GIT workflow.
	+ Pro dodání binárních artefaktů je určena služba Azure DevOps Artifacts.
	+ Základní běhové prostředí všech SW řešení pro projekt ISSI jsou **linuxové** docker kontejnery nasazované do Kubernetes.
	+ Základní prostředí pro dohled a sběr telemetrie všech SW řešení je Azure application insights, ke kterým musí mít přístup členové provozu, vývoje a bezpečnosti, aby se tak předešlo případným neshodám ohledně výkonu a stability řešení. NAKIT předpokládá, že logování a sběr telemetrie probíhá dle best practices, dle jednotlivých SW frameworků použitých pro implementaci.
	+ NAKIT před produkční prostředí (Stage NAKIT) bude ve stejné konfiguraci jako produkční prostředí.
	+ Docker kontejnery musí podporovat non-root běh.
	+ Při vytváření vlastních docker image se musí vycházet z oficiálních, digitálně podepsaných docker image ze služby Docker Hub, nebo oficiálního repositáře Microsoft a během procesu docker build je nutné tyto digitální podpisy kontrolovat.
	+ Používání docker base image jiné, než oficiální je striktně zakázáno.
	+ S každým git commitem musí být spojen ticket v Azure DevOps tak, aby bylo možné identifikovat, kdo a proč modifikoval zdrojové kódy SW řešení. Z těchto ticketů budou automaticky generovány release notes.
	+ Git push do master větve bude zakázán. Společně s partnery bude definován Git workflow (např. jako [Git Workflow](https://www.atlassian.com/git/tutorials/comparing-workflows/gitflow-workflow#%3A%7E%3Atext%3DGitflow%20Workflow%20is%20a%20Git%2Cdesigned%20around%20the%20project%20release)) a jmenováni správci jednotlivých větví pro řešení pull requests. Správci mohou být zaměstnanci NAKIT i programátoři partnerů.
	+ Release build musí probíhat v prostředí NAKIT Azure DevOps a výsledné docker images musí být podepsány klíči NAKIT a uložené v privátním docker repository odkud jsou nasazovány do prostředí Kubernetes.
	+ V kontextu filozofie kultury DevOps jsou všichni členové vývoje a provozu zodpovědní za plynulou kontinuální integraci a kontinuální nasazování SW řešení. Provoz NAKIT připravuje CD/CI pipelines a musí informovat vývojové týmy o procesech automatizace, zprostředkovat logy, spustitelnou dokumentaci neobsahující tajemství (např. Helm šablony pro Kubernetes, ARM šablony pro Azure infrastrukturu apod.) tak, aby byla možná úzká spolupráce a pochopení potřeb a cílů DEV a OPS týmu.
	+ Členové DEV týmu kontinuálně během vývoje udržují verze použitých frameworků a SW knihoven třetích stran v aktuálních stable verzích, aby výsledná SW řešení neobsahovala známé bezpečností díry.
	+ Všechna prostředí v NAKIT (Dev, Test, Stage, Produkce) používají Application Gateway s aktivovanou webovou firewall v blokujícím režimu. DEV tým tak musí implementovat svá řešení v souladu s požadavky OWASP 3.0.
	+ Členové OPS týmu kontinuálně udržují všechna aktiva prostředí i SW řešení např. Kubernetes, Redis, Postgresql, Drupal, apod. v aktuálních stable verzích, aby celé prostředí neobsahovalo známé bezpečnostní díry, nebo neporušovalo ISO 27001 dle reportů Azure security center.

###### Požadavek na platformní služby

Při návrhu nových komponent a funkcí je nutné vždy upřednostňovat platformní Azure služby (PaaS, SaaS), které jsou podporované v datacentrech regionů západní, nebo severní Evropa a jsou pokryty adekvátní úrovní SLA v produkčních prostředích (minimálně 99,9 %).

##### Přístupy administrátorů a vývojářů

Přístup do vývojového, testovacího, před produkčního, stage a produkčního prostředí s administrátorským oprávněním za účelem řešení problémů, které se projeví jako důležité pro ladění problémů je určené jen pro provozovatele – NAKIT, s. p.

Členové DEV týmu budou mít přístupy do prostředí application insights a databází DEV prostředí. Přístupy na stage a produkční prostředí jsou pro členy DEV týmu implicitně zakázány. V případě závažných incidentů v SW řešeních je možné na základě ticketu v Azure DevOps tato prostředí dočasně zpřístupnit pro analýzu chyb. Nicméně správné logování do Application insigts, které umožňuje proaktivní dohled a velmi detailní analýzu chování celého řešení by mělo tyto potřeby eliminovat na minimum.

###### Ochrana proti vnějším útokům

Aplikace musí být chráněny proti nejčastějším útokům, které byly identifikovány nezávislým společenstvím OWASP ([http://www.owasp.org](http://www.owasp.org/)) tím, že se při vývoji použijí principy definované dle této metodiky v aktuálním znění. Pozornost musí být věnována především následujícím zranitelnostem:A01 Broken Access Control

Řízení přístupu prosazuje zásady tak, aby uživatelé nemohli jednat v rozporu se svými určenými oprávněními. Selhání obvykle vede k neoprávněnému vyzrazení informací, modifikaci nebo zničení všech dat nebo k provedení obchodní funkce mimo omezení uživatele. Mezi běžné chyby řízení přístupu patří např:

* Porušení principu nejmenších oprávnění nebo odepření ve výchozím nastavení, kdy by přístup měl být udělen pouze určitým schopnostem, rolím nebo uživatelům, ale je dostupný komukoli.
* Obcházení kontrol řízení přístupu úpravou adresy URL (manipulace s parametry nebo vynucené procházení), interního stavu aplikace nebo stránky HTML nebo pomocí útočného nástroje upravujícího požadavky API.
* Povolení prohlížení nebo úprav cizího účtu poskytnutím jeho jedinečného identifikátoru (nezabezpečené přímé odkazy na objekty).
* Přístup k rozhraní API s chybějícími kontrolami přístupu pro POST, PUT a DELETE.
* Zvýšení oprávnění. Vystupování jako uživatel bez přihlášení nebo vystupování jako správce při přihlášení jako uživatel.
* Manipulace s metadaty, například přehrání nebo manipulace s tokenem řízení přístupu JSON Web Token (JWT) nebo se souborem cookie či skrytým polem manipulovaným za účelem zvýšení oprávnění nebo zneužití zneplatnění JWT.
* Chybná konfigurace CORS umožňující přístup k API z neautorizovaného/nedůvěryhodného prostředí.
* Vynucení procházení ověřených stránek jako neověřený uživatel nebo privilegovaných stránek jako standardní uživatel.

A02 Cryptographic Failures

Nejdříve je třeba určit potřeby ochrany dat při přenosu a v klidu. Například hesla, čísla kreditních karet, zdravotní záznamy, osobní údaje a obchodní tajemství vyžadují zvýšenou ochranu, zejména pokud se na tyto údaje vztahují zákony o ochraně osobních údajů, např. obecné nařízení EU o ochraně osobních údajů (GDPR), nebo předpisy, např. o ochraně finančních údajů, jako je standard PCI Data Security Standard (PCI DSS). U všech takových údajů:

* Jsou některá data přenášena v otevřeném textu? Týká se to protokolů, jako jsou HTTP, SMTP, FTP, které používají také vylepšení TLS, jako je STARTTLS. Externí internetový provoz je nebezpečný. Ověřte veškerý interní provoz, např. mezi load balancery, webovými servery nebo back-end systémy.
* Používají se nějaké staré nebo slabé kryptografické algoritmy nebo protokoly buď ve výchozím nastavení, nebo ve starším kódu?
* Používají se výchozí kryptografické klíče, jsou generovány nebo opakovaně používány slabé kryptografické klíče nebo chybí řádná správa či rotace klíčů? Jsou šifrovací klíče kontrolovány v úložištích zdrojového kódu?
* Není šifrování vynucováno, např. chybí bezpečnostní směrnice nebo hlavičky HTTP (prohlížeče)?
* Je přijatý certifikát serveru a řetězec důvěryhodnosti řádně ověřen?
* Jsou inicializační vektory ignorovány, opakovaně používány nebo nejsou generovány dostatečně bezpečné pro daný kryptografický režim práce? Je používán nezabezpečený režim provozu, například ECB? Používá se šifrování v případech, kdy je vhodnější autentizované šifrování?
* Používají se hesla jako kryptografické klíče, pokud chybí funkce odvození klíče ze základu hesla?
* Používá se pro kryptografické účely náhodnost, která nebyla navržena tak, aby splňovala kryptografické požadavky? I když je zvolena správná funkce, musí ji vývojář nasadit, a pokud ne, přepsal vývojář zabudovanou funkci silného nasazení seedem, který nemá dostatečnou entropii/nepředvídatelnost?
* Používají se zastaralé hashovací funkce, jako je MD5 nebo SHA1, nebo se v případě potřeby kryptografických hashovacích funkcí používají nekryptografické hashovací funkce?
* Používají se zastaralé kryptografické metody vyplňování, jako je PCKS číslo 1 v1.5?
* Jsou kryptografické chybové zprávy nebo informace postranního kanálu zneužitelné, například formou útoků typu padding oracle?

A03 Injection

Aplikace je zranitelná vůči útoku, pokud:

* Uživatelem zadaná data nejsou aplikací ověřována, filtrována nebo upravována.
* Dynamické dotazy nebo neparametrizovaná volání bez kontextového escapování jsou použity přímo v interpretu.
* Nepřátelská data jsou použita v rámci parametrů vyhledávání ORM (object-relational mapping) k získání dalších citlivých záznamů.
* Nepřátelská data se používají přímo nebo se spojují. SQL nebo příkaz obsahuje strukturu a škodlivá data v dynamických dotazech, příkazech nebo uložených procedurách.

Mezi nejběžnější injektáže patří injektáž SQL, NoSQL, příkaz OS, objektově relační mapování (ORM), LDAP a Expression Language (EL) nebo Object Graph Navigation Library (OGNL). Koncept je u všech interpretů shodný. Kontrola zdrojového kódu je nejlepší metodou, jak zjistit, zda jsou aplikace zranitelné vůči injektážím. Důrazně se doporučuje automatizované testování všech parametrů, hlaviček, adres URL, souborů cookie, datových vstupů JSON, SOAP a XML. Organizace mohou do CI/CD pipeline zahrnout nástroje pro statické (SAST), dynamické (DAST) a interaktivní (IAST) testování zabezpečení aplikací, aby identifikovaly zavedené chyby v oblasti injection ještě před produkčním nasazením.

A04 Insecure Design

Nezabezpečený design je široká kategorie představující různé nedostatky, vyjádřené jako "chybějící nebo neúčinný kontrolní design". Nezabezpečený design není zdrojem pro všechny ostatní kategorie rizik Top 10. Existuje rozdíl mezi nezabezpečeným návrhem a nezabezpečenou implementací. Nedostatky v návrhu a implementaci rozlišujeme z určitého důvodu, mají různé příčiny a způsoby nápravy. I bezpečný návrh může mít vady implementace vedoucí ke zranitelnostem, které mohou být zneužity. Nezabezpečený návrh nelze opravit dokonalou implementací, protože potřebné bezpečnostní kontroly nebyly z definice nikdy vytvořeny na obranu proti konkrétním útokům. Jedním z faktorů, které přispívají k nezabezpečenému návrhu, je nedostatečné profilování obchodních rizik, které je vlastní vyvíjenému softwaru nebo systému, a tedy neschopnost určit, jaká úroveň návrhu zabezpečení je nutná.

Shromážděte a projednejte obchodní požadavky na aplikaci s podnikem, včetně požadavků na ochranu důvěrnosti, integrity, dostupnosti a autenticity všech datových aktiv a očekávané obchodní logiky. Vezměte v úvahu, jak bude aplikace vystavena riziku a zda potřebujete oddělení uživatelů (navíc k řízení přístupu). Sestavte technické požadavky včetně funkčních a nefunkčních požadavků na zabezpečení. Naplánujte a vyjednejte rozpočet pokrývající všechny činnosti spojené s návrhem, sestavením, testováním a provozem, včetně bezpečnostních činností.

Bezpečný návrh je kultura a metodika, která neustále vyhodnocuje hrozby a zajišťuje, že kód je robustně navržen a testován tak, aby zabránil známým metodám útoku. Modelování hrozeb by mělo být začleněno do upřesňovacích sezení (nebo podobných činností); hledejte změny v datových tocích a řízení přístupu nebo jiných bezpečnostních kontrolách. Při vývoji uživatelského scénáře určete správné toky a stavy selhání, zajistěte, aby byly dobře pochopeny a odsouhlaseny odpovědnými a dotčenými stranami. Analyzujte předpoklady a

podmínky pro očekávané a chybové toky, ujistěte se, že jsou stále přesné a žádoucí. Určete, jak ověřit předpoklady a prosadit podmínky potřebné pro správné chování. Zajistěte, aby výsledky byly zdokumentovány v příspěvku uživatele (user story). Poučte se z chyb a nabídněte pozitivní pobídky na podporu zlepšení. Bezpečný návrh není doplněk ani nástroj, který můžete přidat do softwaru.

Bezpečný software vyžaduje bezpečný životní cyklus vývoje, určitou formu bezpečného návrhového vzoru, metodiku zpevněné cesty, knihovnu zabezpečených komponent, nástroje a modelování hrozeb. Obraťte se na odborníky na bezpečnost na začátku softwarového projektu v průběhu celého projektu a údržby softwaru. Zvažte využití modelu vyspělosti OWASP Software Assurance Maturity Model (SAMM), který vám pomůže strukturovat vaše úsilí o bezpečný vývoj softwaru.

A05 Security Misconfiguration Aplikace může být zranitelná, pokud:

* Chybí vhodné posílení zabezpečení v kterékoli části aplikačního stacku nebo jsou nesprávně nakonfigurována oprávnění ke cloudovým službám.
* Jsou povoleny nebo nainstalovány nepotřebné funkce (např. nepotřebné porty, služby, stránky, účty nebo oprávnění).
* Výchozí účty a jejich hesla jsou stále povoleny a nezměněny.
* Zpracování chyb odhaluje uživatelům stack traces nebo jiná příliš informativní chybová hlášení.
* U aktualizovaných systémů jsou nejnovější bezpečnostní funkce zakázány nebo nejsou bezpečně nakonfigurovány.
* Nastavení zabezpečení v aplikačních serverech, aplikačních frameworcích (např. Struts, Spring, ASP.NET), knihovnách, databázích atd. nejsou nastavena na bezpečné hodnoty.
* Server neposílá bezpečnostní hlavičky nebo směrnice nebo nejsou nastaveny na bezpečné hodnoty.
* Software je zastaralý nebo zranitelný

A06 Vulnerable and Outdated Components Pravděpodobně jste zranitelní:

* Pokud neznáte verze všech používaných komponent (na straně klienta i serveru). To zahrnuje komponenty, které používáte přímo, i vnořené závislosti.
* Pokud je software zranitelný, nepodporovaný nebo zastaralý. To zahrnuje operační systém, webový/aplikační server, systém správy databází (DBMS), aplikace, rozhraní API a všechny komponenty, běhová prostředí a knihovny.
* Pokud pravidelně nekontrolujete zranitelnosti a neodebíráte bezpečnostní bulletiny týkající se používaných komponent.
* Pokud neopravujete nebo neaktualizujete základní platformu, frameworky a závislosti včas a s ohledem na rizika. To se běžně stává v prostředích, kde je oprava měsíčním nebo čtvrtletním úkolem v rámci řízení změn, čímž se organizace dostávají do situace, kdy jsou dny nebo měsíce zbytečně vystaveny opraveným zranitelnostem.
* Pokud vývojáři softwaru netestují kompatibilitu aktualizovaných, upgradovaných nebo opravených knihoven.
* Pokud nezabezpečí konfigurace komponent.

A07 Identification and Authentication Failures

Potvrzení identity uživatele, ověřování a správa session jsou klíčové pro ochranu před útoky souvisejícími s ověřováním. Slabiny v ověřování mohou nastat, pokud aplikace:

* Umožňuje automatizované útoky, jako je například "credential stuffing", kdy má útočník k dispozici seznam platných uživatelských jmen a hesel.
* Umožňuje útoky hrubou silou nebo jiné automatizované útoky.
* Povoluje výchozí, slabá nebo dobře známá hesla, například "Password1" nebo "admin/admin".
* Používá slabé nebo neúčinné procesy obnovy pověření a zapomenutých hesel, například "odpovědi založené na znalostech", které nelze zabezpečit.
* Používá datová úložiště s prostým textem, šifrovanými nebo slabě hashovanými hesly.
* Má chybějící nebo neúčinné vícefaktorové ověřování.
* Vystavuje identifikátor relace v adrese URL.
* Opakovaně používá identifikátor relace po úspěšném přihlášení.
* Nezneplatňuje správně identifikátory session. Relace uživatele nebo autentizační tokeny (především tokeny jednotného přihlášení (SSO)) nejsou správně zneplatněny během odhlášení nebo období nečinnosti.

A08 Software and Data Integrity Failures

Selhání integrity softwaru a dat souvisí s kódem a infrastrukturou, které nechrání před porušením integrity. Příkladem je situace, kdy aplikace spoléhá na zásuvné moduly, knihovny nebo moduly z nedůvěryhodných zdrojů, úložišť a sítí pro doručování obsahu (CDN). Nezabezpečený CI/CD pipeline může představovat potenciál pro neoprávněný přístup, škodlivý kód nebo kompromitaci systému. A konečně, mnoho aplikací dnes obsahuje funkci automatických aktualizací, kdy jsou aktualizace stahovány bez dostatečného ověření integrity a aplikovány na dříve důvěryhodnou aplikaci. Útočníci by mohli potenciálně nahrát vlastní aktualizace, které by byly distribuovány a spuštěny na všech instalacích. Dalším příkladem je situace, kdy jsou objekty nebo data zakódovány nebo serializovány do struktury, kterou může útočník vidět a modifikovat, je zranitelná nezabezpečenou deserializací.

A09 Security Logging and Monitoring Failures

Tato kategorie má pomoci odhalit, eskalovat a reagovat na aktivní narušení. Bez logování a monitorování nelze narušení odhalit. K nedostatečnému protokolování, detekci, monitorování a aktivní reakci dochází kdykoli:

* Události, které lze auditovat, jako jsou přihlášení, neúspěšná přihlášení a transakce s vysokým objemem, nejsou zaznamenávány.
* Výstrahy a chyby negenerují žádné, nedostatečné nebo nejasné zprávy logu.
* Protokoly aplikací a rozhraní API nejsou monitorovány z hlediska podezřelých aktivit.
* Protokoly jsou ukládány pouze lokálně.
* Nejsou zavedeny vhodné prahové hodnoty pro upozornění a procesy eskalace reakce nebo nejsou účinné.
* Penetrační testy a skenování pomocí nástrojů pro dynamické testování bezpečnosti aplikací (DAST) (například OWASP ZAP) nevyvolávají výstrahy.
* Aplikace nemůže detekovat, eskalovat nebo upozorňovat na aktivní útoky v reálném čase nebo téměř v reálném čase.

Jste zranitelní vůči úniku informací tím, že události protokolování a výstrah jsou viditelné pro uživatele nebo útočníka.

A10 Server Side Request Forgery (SSRF)

K chybám SSRF dochází vždy, když webová aplikace načítá vzdálený prostředek bez ověření uživatelem zadané adresy URL. Útočník tak může aplikaci přimět k odeslání vytvořeného požadavku na neočekávané místo určení, a to i v případě, že je chráněna bránou firewall, sítí VPN nebo jiným typem řízení přístupu (ACL).

Vzhledem k tomu, že moderní webové aplikace poskytují koncovým uživatelům pohodlné funkce, stává se načítání adresy URL běžným scénářem. V důsledku toho se zvyšuje výskyt SSRF. Také závažnost SSRF je stále vyšší v důsledku cloudových služeb a složitosti architektur.

Kromě aktuálních OWASP TOP10 je třeba věnovat pozornost také zranitelnostem, které se v tomto žebříčku umístily v minulých letech.

* XML External Entities (XXE): Mnoho starších nebo špatně nakonfigurovaných procesorů XML vyhodnocuje odkazy na externí entity v dokumentech XML. Externí entity mohou být použity k odhalení interních souborů pomocí jejich URI, interního sdílení souborů, skenování interních portů, vzdálenému spuštění kódu a útokům typu Denial of Service.
* Cross-Site Scripting XSS: K chybám XSS dochází vždy, když aplikace zahrne nedůvěryhodná data do nové webové stránky bez řádné validace nebo escapování nebo aktualizuje existující webovou stránku s daty poskytnutými uživatelem pomocí rozhraní API prohlížeče, které může vytvářet HTML nebo JavaScript. XSS umožňuje útočníkům spustit v prohlížeči oběti skripty, které mohou unést uživatelské relace, poškodit webové stránky nebo přesměrovat uživatele na škodlivé stránky.
* Cross Site Request Forgery: CSRF je technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit.
* Nezabezpečené přesměrování: Využívá nezabezpečených přesměrování v aplikacích (redirect a froward) k tomu, aby z důvěryhodné stránky přesměrovala nic netušícího uživatele na stránku škodlivou.

Aplikace nesmí obsahovat žádné zranitelnosti, které jsou klasifikované jako střední, vysoké a kritické. O závažnosti jednotlivých zranitelností rozhoduje bezpečnostní manažer NAKIT.

###### Pravidla XML komunikace

Při použití XML komunikace by měly být prováděné tyto kontroly:

* + - Početní a délkové limity:
			* maximální počet atributů v elementu
			* maximální počet namespaces, namespace prefixů a obecně všech lokálních jmen v XML dokumentu
			* maximální délka jména elementu
			* maximální délka jména atributu
			* maximální délka identifikátoru namespace (URI)
		- Znakové sady:
			* konzistence deklarací (atribut „charset“ v HTTP request hlavičce „Content-Type“, BOM na začátku dat a atribut „encoding“ v hlavičce XML)
			* přítomnost netisknutelných znaků
		- Escaping:
			* escaping validních znaků (např. „&#x41;“ místo „A“, též např. „&#x42f;“ místo „Я“, pokud je použitý encoding některý z UTF apod.)
			* použití znaku „&“ mimo escape sekvenci
			* použití znaků „““ (uvozovky – ASCII 34), „’“ (apostrof – 39), „<“ a „>“ mimo místa, kde mají syntaktický význam
			* kontrola správného ohraničení CDATA sekcí (pokud se vůbec mohou vyskytovat, pokud ne, tak rovnou odmítat XML zprávy, které CDATA obsahují)
		- Přítomnost XML External Entity v DTD

###### JSON formát

Při použití JSON formátu pro výměnu externích dat (neplatí pro API v aplikaci) by měly být prováděné minimálně tyto kontroly:

* + - maximální velikost zprávy
		- maximální délka názvu klíče
		- neunikátní klíče
		- maximální počet elementů
		- maximální úroveň vnoření
		- maximální velikost pole (myšleno array, nikoli field)
		- komentáře, pokud jsou zakázané nebo limitované velikostí
		- limit objemu whitespace (tabulátory, mezery, odřádkování)
		- kontrola striktní syntaxe a struktury JSON dokumentu (některé parsery v aplikacích

ledacos tolerují)

* + - kontrola kanonické formy nebo provedení kanonizace (pokud je požadována)
		- kontrola obsahu (jména klíčů, hodnoty) na sekvence XSS či SQLi (s možností vypnout per element – nemusí být datově transparentní a někdy může hodnota naopak záměrně obsahovat renderované HTML)
		- provádí se kontrola syntaxe kódu JSON – parser pro RFC4627
		- validace key value, metoda zjišťuje, zda hodnoty použité v key value odpovídají typu definované hodnoty (numeric,boolean apod.)

##### Pravidla logování

Základní prostředí pro dohled a sběr telemetrie všech SW řešení jsou Azure application insights, ke kterým musí mít přístup členové provozu, vývoje a bezpečnosti, aby se tak předešlo případným neshodám ohledně výkonu a stability řešení.

Projekty mohou využívat např. Google analytics pro vyhodnocování chování uživatelů na webových portálech. Google analytics se nesmí používat v privátní transakční části systému.

NAKIT předpokládá, že logování a sběr telemetrie probíhá dle best practices dle jednotlivých SW frameworků použitých pro implementaci SW řešení.

Logování SW řešení dodávaných partnery by se mělo nést v duchu, že logy jsou psány pro potřeby oddělení provozu a bezpečnosti (nikoli pouze pro debuggovací potřeby programátorů). Všichni členové týmu vývoje, provozu i bezpečnosti musí na základě informace z logu identifikovat a vyřešit problém.

Neošetřené výjimky, nebo informace v logu typu „došlo k neočekávané chybě“, ačkoli programátor mohl a měl specifikovat konkrétní chybu např. nedostupnosti prostředí třetích stran, vypršení certifikátu, nevalidní vstupní data apod, je projevem nekvalitního exception handlingu a NAKIT může vyzvat subdodavatele k nápravě.

Umožnit nastavení úrovně logování – například:

* Verbose, Debug, Info, Warn, Error, Fatal

Součástí logování musí být partnery definovaná a NAKIT předaná politika exception handling hlavně z důvodu, aby obsahem logů na produkci nebyla data obsahující tajemství (např. hesla, šifrovací klíče, emailové adresy, a další atributy citlivé dle GDPR).

Pokud existují záznamy, které je nutné logovat a zároveň podléhají GDPR je nutné tyto aspekty definovat v politice logování a exception handling a poskytnout členům OPS týmu tak, aby proces NAKIT popsal způsoby bezpečného ukládání a zpracování takovýchto informací.

Soupis specifických ID možných chyb s popisem musí být součástí programátorské dokumentace kontinuálně předávané členům OPS týmu.

##### Požadavky na zaznamenávání událostí, jeho uživatelů a administrátorů

1. Jednoznačnou síťovou identifikaci zařízení původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci.
2. Sběr informací o bezpečnostních a provozních událostech; zejména zaznamenává:
	* datum a čas včetně specifikace časového pásma
	* typ činnosti
	* identifikaci technického aktiva, které činnost zaznamenalo
	* jednoznačnou identifikaci účtu, pod kterým byla činnost provedena
	* jednoznačnou síťovou identifikaci zařízení původce a
	* úspěšnost nebo neúspěšnost činnosti
3. Ochranu informací získaných podle písmen a) a b) před neoprávněným čtením a jakoukoli změnou.
4. Zaznamenávání:
	* přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů
	* činností provedených administrátory
	* úspěšné i neúspěšné manipulace s účty, oprávněními a práv
	* neprovedení činností v důsledku nedostatku přístupových práv a oprávnění
	* činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému
	* zahájení a ukončení činností technických aktiv
	* kritických i chybových hlášení technických aktiv
	* přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech

a změny nastavení nástrojů pro zaznamenávání událostí

Logy se ukládají v prostředí Azure Log analytics po dobu 18 měsíců a jsou zároveň zasílány do DCeGOV (Dohledové centrum eGovernmentu).

##### Dokumentace

* 1. ***Dokumentace při vytvoření díla***

##### Bezpečnostní politika

* + - * musí být v souladu s VyKB
			* musí být v souladu s požadavky ISMS MV

###### Dokumentace k integraci řešení

* datové toky
* použité protokoly
* architektonický nákres komponent a jejich spolupráce
* diagram logického a fyzického zapojení

###### Systémová příručka

* Popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností v informačním systému veřejné správy a návod na používání těchto funkcí.
* Parametry kvality vycházejí z požadavků na kvalitu.
* Podrobný popis IS nebo odkaz na dokument, ve kterém je popis uveden.
* Popis jednotlivých činností vykonávaných při správě IS, včetně činností definovaných pro role, určení fyzických osob, které tyto činnosti vykonávají a oprávnění nezbytných pro výkon těchto činností.
* Definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání aplikace.

###### Uživatelské příručky

* Uživatelská příručka

###### Provozní deník

Provozní deník je vedený v Azure DevOps v podobě ticketu typu service book.

###### Systém řízení dokumentů a záznamů

Provádí se dle **ISMS 02.03.01 Řízení dokumentů a záznamů**

##### Zdrojový kód

Součástí dokumentace SW řešení je i vývojářská dokumentace v podobě doplňujících komentářů uvnitř funkcí, metod a popisů tříd.

Každý z programátorských jazyků má své best practice ohledně pojmenovávání tříd, atributů, názvu tříd a proměnných i postupů při programátorské dokumentaci. Společně s partnery budou tyto best practice kodifikovány jakožto závazné postupy dokumentace a tvorby SW.

Komentáře jsou součásti [syntaktických](https://cs.wikipedia.org/wiki/Syntaktick%C3%A1_anal%C3%BDza) pravidel zápisu programu v mnoha [programovacích](https://cs.wikipedia.org/wiki/Programovac%C3%AD_jazyk) [jazycích](https://cs.wikipedia.org/wiki/Programovac%C3%AD_jazyk). Komentář se vkládá před nebo za část [zdrojového kódu](https://cs.wikipedia.org/wiki/Zdrojov%C3%BD_k%C3%B3d) (např. příkaz, metodu, třídu), jehož funkci nebo význam je potřeba vysvětlit. Používání komentáře není povinné, umožňuje však napomoci k pochopení činnosti [programu](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_program). Komentář nemá popisovat, co program dělá (protože to vyplývá ze zápisu programu), ale proč to dělá. Komentáře obecně mohou velmi usnadnit pochopení činnosti programu, mohou mít samo-dokumentující funkci. Syntaxe a pravidla pro přidávání komentářů budou dle konkrétního programovacího jazyka.

Kromě komentářů ve zdrojových kódech je zdrojový kód rovněž navázán na vývojářskou dokumentaci, obsahující popis konceptu a fungování každého bloku, tj. zdrojový kód každé komponenty je identifikován v příslušném schématu a popisu ve shodné jmenné konvenci.

Dokumentace rovněž obsahuje:

* podrobný popis konfiguračních parametrů vč. jejich formátu
* popis použitých API
* popis vazeb mezi jednotlivými komponentami
* seznam chybových kódů a jejich význam
* další nezbytné prvky, jako např. certifikáty, šifrovací klíče, logované údaje Požadavky na vývoj:
* Vyvíjená komponenta / aplikace musí splňovat požadavky Cloud native.
	+ Definice cloud native: [Defining Cloud Native | Microsoft Docs](https://docs.microsoft.com/en-us/dotnet/architecture/cloud-native/definition)
	+ Oficiální popis Cloud native nadace Cloud native computing foundation: [CNCF](https://github.com/cncf/foundation/blob/master/charter.md)
* Konfigurační soubory a tajemství nejsou součástí zdrojového kódu ani databáze. Předávají se do běhového prostředí přes environment variables
* Certifikáty a hesla jsou uloženy v chráněném úložišti (např. Kubernetes secrets, Azure key vault, apod.).
* Soubory (dokumenty, přílohy apod.) se neukládají do transakční databáze.
* U nových komponent / aplikace jsou součástí dodávky zdokumentovány Unit testy.
* Součástí dodávky jsou FAT testy a jejich výsledky.
* Každý kontejner / mikroslužba musí obsahovat API pro Kubernetes readiness a liveness probes.
* Sběr telemetrie přes Azure application Insights probíhá od prvních řádek kódu.
* Vyvíjené komponenty jsou multilplatforní a docker images musí podporovat non-root běh.
* Každá komponenta má healt-check pro její dohled a je implementován jako REST volání.

##### Pravidla a chování Git, obecný flow vývoje

Projekt manažer nebo produkt manažer pravidelně aktualizuje plán release.

Ke každé release oddělení testování vytváří testovací protokol a uloží na SHP NAKIT. Požadavky na zřízení přístupu do Azure DevOps se zasílají na PM.

###### Nové požadavky

Na základě požadavků MV projektový, nebo produktový manažer zřizuje v Azure DevOps tickety typu **Epic, Feature, Enhacement**. Epic slouží pro velké požadavky, který je dále rozdělen na jednotlivé **Feature.**

Jednotlivé požadavky jsou předány k vytvoření zadání a jsou ve stavu **Analyse.** Po vyjasnění zadání a provedení připomínkovacího řízení, PM požadavek předá k provedení odhadů pracnosti team leaderům a team leaderu subdodavatele. Po schválení od MV, PM požadavek zařadí do release plánu (plánované iterace) a předán subdodavateli. Subdodavatel potvrdí převzetí v release a nastaví jeho stav na **Active.** Po vyřešení a vložení zdrojového kódu do GITu, nastaví subdodavatel jeho stav na **Resolved**. Provozní podpora po schválení nasazení nasadí do prostředí DEV, nastaví stav na **ToTest** a přiřadí na vedoucího oddělení testování NAKIT, který přiřadí na konkrétního testera.

Po úspěšném otestování v prostředí **DEV**, tester nastaví stav chyby na **Tested DEV.** V případě chyby tester vrátí řešiteli a nastaví stav na Active.

PM po rozhodne o nasazení na Stage, provozní podpora nasadí na Stage a rozešle informaci, že je nová verze na Stage nasazena k testování Po úspěšném otestování v prostředí Stage, tester nastaví stav na **Tested Stage**. V případě chyby tester vrátí řešiteli a nastaví stav na **Active.**

Po nasazení do produkce a úspěšném otestování v produkčním prostředí, tester nastaví stav na **TestedProd**. V případě chyby tester vrátí řešiteli a nastaví stav na **Active.** PM po nasazení do produkce zkontroluje obsah release na nastaví na stav **Close.**

* 1. ***Řešení nahlášených incidentů***

##### Zaevidování chyby

Chyby v **produkci** zaslané na email zaeviduje služba podpory provozu v Azure DevOps označí štítkem **PROD**, do názvu tiketu uvede: „Zkratku názvu projektu “\_“Zkratku prostředí“**:** Vyplní vždy kategorii (A, B, C, D), Device description (jeli známo) a číslo release. Dle povahy chyby předá na teamleadera řešitelů.

Chyby z **vývoje** zaslané na email, například z MV ČR, zaeviduje podpora provozu v Azure DevOps označí štítkem prostředí (DEV/ Stage), do názvu tiketu uvede **ISSI\_DEV** nebo **Stage**. Dále vyplní device description a kategorii chyby. **Dále bude uvedeno, jestli chyba vznikla neotestováním u partnerů při vývoji.** Dále musí být vyplněno Related, určení tasku, se kterým souvisí. Chyby zjištěné oddělením testování NAKIT testeři zaevidují v Azure DevOps s vyplněním všech atributů. Všechny chyby jsou nejdříve přiděleny na PM. PM přidělí k řešení.

Chyba je ve stavu **New**.

##### Proces odstraňování chyby

Řešitel převezme chybu a nastaví její stav na **Analyse**.

Po vyřešení chyby, kdy dojde k nastavení parametrů nebo release nastaví stav na **Resolve**. V případě, že je nutné nasadit opravu je nutné zaslat informaci na OPS tým Nakit. Provoz nasadí na DEV a po nasazení nastaví chybu do stavu **To Test** a přiřadí na testera.

Po úspěšném otestování v prostředí DEV, tester nastaví stav chyby na **Tested DEV**. V případě chyby tester vrátí řešiteli a nastaví stav na **Active.**

Po úspěšném otestování v prostředí Stage, tester nastaví stav chyby na **Tested Stage.**

V případě chyby tester vrátí řešiteli a nastaví stav na **Active.**

Po nasazení do produkce a úspěšném otestování v prostředí, tester nastaví stav chyby

na **Close**. V případě chyby tester vrátí řešiteli a nastaví stav na **Active.**

##### Workflow odstranění chyby



###### Změnové požadavky

Zadávat vlastní nápady na vylepšení, které neprošli nějakým všeobecným odsouhlasením, jsou zadané jako **Issue** do Azure DevOps a jsou přiřazené na Projektového/Produktového manažera.

Postup:

1. Pokud se nápad **neodsouhlasí**, Projektový/Produktový manažer napíše komentář k **Issue**

proč a zavře jej – stav **CLOSED**.

1. Pokud se nápad **odsouhlasí:**
	1. Projektový/produktový manažer Issue přenastaví na typ **Enhacement**, změní stav na

**ANALYSE** a přiřadí jej na analytika.

* 1. Analytik projde případné další souvislosti a bude-li třeba, dopíše analýzu. Provede připomínkové řízení a po vypořádání připomínek předá na PM.
	2. PM provede nacenění, odsouhlasení vlastníka systému a zařazení do verze. Další postup dle kapitoly [6.1](#_bookmark0) této přílohy - „Nové požadavky“.

###### Dodržování jmenné konvence v Azure DevOps

TITLE=název – Chceme mít možnost je filtrovat podle kategorií. První slovo dle jednotlivých bodů rozdělení. Druhé slovo bude oblast v projektu, abychom to dobře roztřídili /důležité je nedělat překlepy/. To je důležité hlavně u požadavků, které se nebudou řešit hned. Prostředí bude v názvu požadavku specifikováno pouze pokud se bude jednat o

TEST prostředí nové ISSI (např. testování formuláře metodiky).

**Např.** nový ISSI: TEST-Formuláře-metodika chybný odkaz

V detailu popisku požadavku bude vložena vždy URL adresa stránky, na které se bug/enhancement vyskytl.

##### Unit testování a pravidla přístupnosti

V souladu s normou WCAG 2.1, a zákonem č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací a o změně zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů.

Kontroluje dodavatel front endu a vždy s každou release potvrdí, že je release v souladu s pravidly.

##### Bezpečnost

* 1. ***Bezpečný vývoj***
		1. **Minimální bezpečnostní požadavky na vývoj aplikací z hlediska jejich kritičnosti**

Při vývoji softwarové aplikace musí být splněna řada bezpečnostních opatření, která mají vliv zajištění vysokého stupně důvěrnosti, dostupnosti a integrity informací v nich obsažených. Externí dodavatelé i interní vývoj musí splnit sadu opatření obsažených ve standardu [OWASP Application Security Verification Standard](https://owasp.org/www-project-application-security-verification-standard/). Představuje seznam požadavků či testů z oblasti aplikační bezpečnosti, který je využitelný architekty, vývojáři, testery, bezpečnostními specialisty, výrobci nástrojů a uživatele (konzumenty) aplikací pro definování, vývoj a testování bezpečných aplikací.

Požadavky jsou členěny do 14 sekcí, kdy jednotlivé požadavky jsou doporučeny pro aplikace s nízkým (L1), středním (L2) a vysokým dopadem či hodnotou (L3) pro zákazníka.

Zmíněné oblasti požadavků ve standardu:

* + - 1. Ověřovací požadavky na architekturu, návrh a modelování hrozeb
			2. Ověřovací požadavky na autentizaci
			3. Ověřovací požadavky na správu relací
			4. Ověřovací požadavky na řízení přístupu
			5. Ověřovací požadavky na validaci, ošetřování a kódování
			6. Ověřovací požadavky na uloženou kryptografii
			7. Ověřovací požadavky na řízení chyb a logování
			8. Ověřovací požadavky na ochranu dat
			9. Ověřovací požadavky na komunikace
			10. Ověřovací požadavky na škodlivý kód
			11. Ověřovací požadavky na business logiku
			12. Ověřovací požadavky soubory a zdroje
			13. Ověřovací požadavky na API a webové služby
			14. Ověřovací požadavky na konfigurace

Dodavatel bude při vývoji, testování a nasazení aplikace naplňovat doporučené požadavky dle definované kritičnosti vyvíjené aplikace (L1, L2 nebo L3).

Každá vyvíjená softwarová aplikace musí splňovat specifické náležitosti a postupy během jejího vývoje. Detail a záběr bezpečnostních požadavků v každé fázi se odvíjí od míry citlivosti či kritičnosti dané aplikace.

Aplikace lze z pohledu potenciálního negativního dopadu při narušení bezpečnosti klasifikovat do 3 kategorií.

1. Kritická (L3) – významná aplikace, jejíž nedostupnost, narušení integrity nebo důvěrnosti by ohrozilo reputaci organizace nebo by plynuly významné finanční postihy. Aplikace nakládá s citlivými, osobními či jinak strategickými údaji a jejich ohrožení (zcizení, zveřejnění) může narušit chod (většiny) klíčových business procesů organizace. Je třeba klást nejvyšší možná bezpečnostní opatření na takovou aplikaci v oblasti důvěrnosti, integrity a dostupnosti.
2. Střední (L2) – aplikace, která nakládá s částečně citlivými či strategickými informacemi, jejichž zveřejnění bych vzhledem k povaze či kvantitě neohrozilo významným dopadem chod organizace či některého business procesu. Narušení její důvěrnosti, integrity nebo dostupnosti bude mít dopad na některé klíčové procesy,

ale bez kritického dopadu na chod celé organizace či ohrožení reputační nebo finanční stability.

1. Základní (L1) – aplikace, která nenakládá s citlivými ani strategickými informacemi a nemá dopad na chod organizace. V případě narušení její důvěrnosti, integrity nebo dostupnosti se to nijak nedotkne klíčových procesů, pouze podpůrných s méně zřejmým přímým vlivem na hlavní procesy.
	* 1. **Praktiky a zásady bezpečného vývoje a standardy při programování**
* Aplikace standardů a konvencí – Jakmile budou přijata rozhodnutí o použitých technologiích, musí být vytvořeny, udržovány a sděleny příslušné vývojové standardy a konvence, které podporují jak psaní bezpečného kódu, tak opětovné použití vestavěných bezpečnostních funkcí a schopností.
* Používejte opakovaně vestavěné funkce zabezpečení ve vybraných vývojových frameworcích a nástrojích a zajistěte, aby byly ve výchozím nastavení zapnuté. To pomůže všem vývojářům řešit známé třídy problémů, a to systémově nikoli dle individuálního uvážení.
* Jakékoli použití frameworků / knihoven / komponent by mělo být v co nejmenší míře spojeno, aby je bylo možné v případě potřeby snadno vyměnit / upgradovat.
* Standardy musí být vynutitelné a realizovatelné
* Maximálně automatizujte revize kódu na zranitelnosti pro zefektivnění a zrychlení kontroly (minimálně v rozsahu OWASP Top 10)
	+ 1. **Bezpečné funkce**
1. Zajistěte předpis (ne)povolených a kontrolu použitých funkcí dle použitého jazyka (Java, PHP, .NET) včetně doporučených ekvivalentů k těmto funkcím. Některé dynamické jazyky používají nebezpečné funkce generované v rámci běhové prostředí a jsou zdrojem zranitelností ([referenční seznam CWE Top 25](https://cwe.mitre.org/top25))
2. Využívejte statické analyzátory kódu, případně nástroje typu RASP (Runtime application self-protection), které mají kontextový vhled do volání funkcí uvnitř běžící aplikace. RASP zvyšuje bezpečnost softwaru sledováním jeho vstupů a blokováním těch, které by mohly umožnit útok, a zároveň chrání runtime prostředí před nežádoucími změnami a

neoprávněnými zásahy. Chráněné aplikace spoléhají méně na externí zařízení, jako jsou firewally, aby poskytovaly ochranu zabezpečení v běhovém prostředí. RASP může být integrován jako framework nebo modul běžící ve spojení s programovým kódem, knihovnami a systémovými voláními.

1. Další metodou ochrany před zanesením kódu je integrace analyzátoru přímo do IDE nebo kontroly v rámci CI/CD při sestavování aplikace.
2. Používejte aktuální verze kompilátoru a nástrojů vývojové linky a bezpečné předvolby kompilátoru (např. ochrana před buffer overruns a underruns v podobě ochrany při kompilaci a v běhovém prostředí proti chybám poškození paměti)
	* 1. **Bezpečné nakládání s daty**
* Všechny uživatelské vstupy musí být považovány za nedůvěryhodné, proto využívejte striktní validaci vstupů od klienta, parametrizujte dotazy do databáze. Každá vrstva aplikační architektura by měla mít svou vlastní ochranu
* Kromě validace vstupů zvažte dle využitého kontextu vynutitelnost segregace dat, čímž zamezíte, aby se data stala součástí aplikační logiky
	+ - 1. Kódování, které zajišťuje, že data jsou transformována tak, aby byla interpretována čistě jako data v kontextu, kde se používají
			2. Data binding zabraňuje interpretaci dat v podobě kontrolní logiky svázáním se specifickým datovým typem
* Jako prevenci před obejitím některých bezpečnostních filtrů zvažte použití kanonizace. Při rozhodování o bezpečnosti uživatelských vstupů by mělo být veškeré dekódování (decode) provedeno nejprve pomocí příslušných API, dokud nebude vyřešeno veškeré kódování (encode). Dále musí být vstup kanonizován a poté validován. Vstup po kanonizaci by měl být ověřen a buď přijat, nebo odmítnut. Teprve po kanonizaci může být učiněno rozhodnutí.
* Vstup z nedůvěryhodných zdrojů by měl být vždy ošetřen, a pokud jsou k dispozici, měly by být použity metody ošetření a validace poskytované komponentami, protože ošetření vytvořená na míru mohou často přehlédnout skryté složitosti.
	+ 1. **Řízení bezpečnostních rizik souvisejících s komponentami třetích stran**

Použité komponenty třetích stran musí projít evidencí a kontrolou minimálně v tomto rozsahu:

* Vést seznam použitých komponent s unikátně identifikovaným číslem komponenty
* Vyhodnotit bezpečnostní rizika vůči známým zranitelnostem
* Zmírněte riziko aktualizacemi, záplatami nebo náhradou komponenty, popřípadě přijměte riziko
* Monitorujte změny a nové zranitelnosti, které se mohou u použitých komponent vyskytovat
	+ 1. **Testování a validace kódu**

Využívejte maximálně automatizované testování za podpory kombinace nástrojů typu:

* Static Analysis Security Testing (SAST) - kontrola nedostatků zdrojového kódu nebo kompilovaného mezijazyka nebo binární komponenty. Hledá známé problematické vzory v kódu založené pouze na aplikační logice, nikoli na chování aplikace při jejím spuštění
	+ Kontrola na výskyt zranitelností během sestavování aplikace nebo rovnou během psaní kódu
	+ SAST nepokrývá detekci zranitelností v business logice, problémy zavedené na více úrovních aplikace nebo třídy problémů vytvořené za běhu.
* Dynamic Analysis Security Testing (DAST) - testování předpřipravených útoků vůči plně běžící (kompilované) aplikaci s veškerou integrací potřebných komponent (podpora testování aplikace napsané i v jazyce nepodporovaném SAST nástrojem nebo v případech kdy aplikace využívá externích volání webových služeb nebo Javascript knihoven uložených mimo repozitář kódu)
* Fuzzing - mnohonásobné variabilní generování nebo mutace dat a jejich předání aplikačním data parserům (síťové protokoly, souborové, IPC). Dobré pokrytí kontroly kódu, zejména pro C, C++
* Software composition analysis (SCA) - zabývá se správou používání komponent s otevřeným zdrojovým kódem. Nástroje SCA provádějí

automatické skenování kódové základny aplikace včetně souvisejících artefaktů, jako jsou kontejnery a registry, s cílem identifikovat všechny komponenty s otevřeným zdrojovým kódem, údaje o jejich souladu s licencemi a případné bezpečnostní zranitelnosti.

* K ověřování konfigurací a zmírnění rizik provozních platforem – využívejte ochranu před útoky na bázi mitigací OS:
	+ ASLR (Address Space Layout Randomization)
	+ DEP (Data Execution Prevention)
	+ CFG (Control Flow Guard)
	+ Služby a nástroje ověřující že webová stránka podporuje záhlaví HTTP související s bezpečností, jako jsou x-frame-options, politika zabezpečení obsahu, HSTS, zabezpečené a http Only cookie flagy, a že konfigurace SSL / TLS na serveru je bez nepodporovaných a zranitelných / nepodporovaných verzí protokolu a šifrovacích sad.
* Automatické funkční testování bezpečnostních požadavků a vlastností aplikace
	+ Rozšiřte standardní unit testy o testování bezpečnostních vlastností stejně jako testujete standardní funkční vlastnosti aplikace.

###### Penetrační testy

(provádění penetračních testů není předmětem plnění, ledaže je tak výslovně stanoveno)

Provádění bezpečnostních testů se řídí § 25 VyKB. Bezpečnostní testy (vulnerability) testy je pak v souladu s výše uvedeným paragrafem nutné provést v souvislosti s významnou změnou podle § 11 odst. 3 VyKB. Při změně bude kompetentní osobou nebo garantem expertně posouzeno, jestli změna má dopad do aktiv nebo nepředstavují pro systém riziko.

Požadavky na Penetrační testování webové aplikace:

* Manuální testování všech požadavků a odpovědí mezi prohlížečem a cílovou aplikací.
* Manipulace se server-side a client-side komponenty aplikace.
* Manipulace s parametry dotazů s cílem přečíst chráněná data z databází (využití SQLi).
* Útoky pomocí Cross-site Request Forgery (CSRF).
* Využití Cross-site Scriptingu (XSS) k převzetí kontroly nad klientskou částí aplikace.
* Obejití sanitace souborů při uploadu k distribuci malwaru na server, například s cílem získat neoprávněný přístup k adresářům a souborům.
* Zneužití slabých procesů pro obnovu hesel, stále aktivní výchozí a testovací účty.
* Odposlech nezabezpečené komunikace serveru s klientem, vyhledávání nechráněných souborů, nešifrovaných záloh.

##### 9. Zkratky, pojmy, definice

Tabulka 1 – Seznam zkratek

|  |  |
| --- | --- |
| **Azure** | Cloudová platforma v datových centrech Microsoftu |
| **Cl/CD pipeline** | Představuje sérii kroků, které je nutné provést, pro správné dodání nové verze softwaru |
| **Git** | je v informatice distribuovaný systém správy verzí vytvořený Linusem Torvaldsem pro vývoj jádra Linuxu |
| **INSPIRE** | Národní geoportál |
| **ISMS** | Systém řízení bezpečnosti informací (Information Security Management Systém) |
| **ISSI** | Informační systém pro veřejné služby a služby veřejné správy INSPIRE |
| **NAKIT** | Národní agentura pro komunikační a informační technologie, s. p. |
| **MV** | Ministerstvo vnitra České republiky |
| **OWASP** | Open Web Application Security Project |
| **PM** | Projektový manažer |
| **SW** | Software |