Smlouva o dodávce SW pro zajištění služeb certifikační autority PostSignum

Číslo 2025/08695

Česká pošta, s.p.

se sídlem:	Politických vězňů 909/4, 225 99 Praha 1
IČO:	47114983
DIČ:	CZ47114983
zastoupen:	Mgr. Vlastimilem Hallou, MBA, ředitelem úseku generálního ředitele
zapsán v obchodním rejstříku u:	Městského soudu v Praze, oddíl A, vložka 7565
bankovní spojení:	[redacted]

(dále jen „**Objednatel**“)

a

MONET+,a.s.

se sídlem:	Za Dvorem 505, 763 14 Zlín - Štípa
IČO:	26217783
DIČ:	CZ26217783
zastoupena:	Ing. Břetislavem Endrysem, předsedou představenstva a Ing. Janem Vavrysem, členem představenstva
zapsána v obchodním rejstříku u:	Krajského soudu v Brně, oddíl B, vložka 3351
bankovní spojení:	[redacted]

dále jako „**Dodavatel**“

dále jednotlivě jako „**Smluvní strana**“ a společně jako „**Smluvní strany**“ uzavírají v souladu s ustanovením § 1746 čl. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“) a zákonem, č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), tuto Smlouvu o dodávce SW pro zajištění služeb certifikační autority PostSignum (dále jen „**Smlouva**“).

Preambule

Objednatel provedl zadávací řízení k nadlimitní veřejné zakázce „SW pro zajištění služeb certifikační autority PostSignum“ (dále jen „**Zadávací řízení**“) na uzavření této Smlouvy. Tato Smlouva je uzavřena s Dodavatelem vybraným 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.

1 Účel a předmět Smlouvy

1.1 Účelem této Smlouvy je zajištění dodávky SW pro vydávání a zneplatňování kvalifikovaných a komerčních certifikátů, publikování CRL (Certificate Revocation List) a zajištění služby OCSP (Online Certificate Status Protocol), jeho údržby a podpory. Tento SW nahradí stávající SW UNICERT od společnosti Verizon.

1.2 Předmětem této Smlouvy je závazek Dodavatele poskytnout:

a) časově neomezené licence pro SW pro zajištění služeb certifikační autority PostSignum (dále jen „**SW**“ nebo, „**Licence**“) včetně implementace SW dle specifikace uvedené v Přílohách č. 1 a 2 Smlouvy;

b) **technickou podporu a údržbu SW** (dále jen „**Podpora**“);

(plnění dle odst. 1.2 Smlouvy společně také jen „**Plnění**“).

1.3 Dodavatel se zavazuje poskytnout Plnění ve sjednaném čase, rozsahu a sjednaným způsobem. Dodavatel se zavazuje poskytnout Plnění v provedení a jakosti odpovídající aktuálnímu stavu technologického vývoje v dané kategorii produktů, jakož i požadavkům Objednatele vymezeným v přílohách Smlouvy. Dodavatel převede vlastnické právo k hmotným složkám Plnění na Objednatele.

1.4 Objednatel se tímto zavazuje Plnění poskytnuté v souladu se Smlouvou převzít a zaplatit za něj sjednanou cenu dle čl. 3 Smlouvy.

1.5 Po uzavření Smlouvy sdělí Objednatel Dodavateli evidenční číslo pro účely fakturace Plnění.

1.6 Pro potřeby plnění této smlouvy platí, že pro poskytování Plnění dle odst. 1.2 písm. b) Smlouvy se použijí Všeobecné obchodní podmínky pro poskytování služeb Objednatele a pro poskytování Plnění dle odst. 1.2 písm. a) Smlouvy se použijí Všeobecné obchodní podmínky pro dodávky zboží Objednatele (dále jen společně jako „**VOP**“). VOP tvoří Přílohu č. 5 této Smlouvy.

2 Podpora

2.1 Podpora podle odst. 1.2 písm. b) této Smlouvy zahrnuje následující plnění:

a) Aktualizace SW nasazením vyšší verze (upgrade SW) včetně zajištění odpovídajících licencí;

b) automatické průběžné bezpečnostní aktualizace SW;

c) poskytování a nasazení opravných patchů, service packů a hotfixů;

d) řešení incidentů včetně odstraňování vad, chyb a vadných či nestandardních stavů (dále jen „**vady**“) SW;

e) poskytnutí opravených verzí SW včetně zajištění odpovídajících licencí;

f) provozování kontaktní hot-line;

g) účast na kontrolních dnech a jednáních týkajících se podpory systému.

2.2 Dodavatel je povinen poskytovat Podporu v pracovních dnech (tj. mimo soboty, neděle a státní svátky) v čase 8:00 – 16:00 hodin po celou dobu účinnosti Smlouvy.

2.3 Kontakt na helpdesk (hot-line) Dodavatele je uveden v odst. 12.1 písm. f) této Smlouvy. Za dostupný helpdesk se považuje i případ, kdy bude možné zanechat vzkaz na záznamníku, nebo odeslat požadavek e-mailem, aniž by bylo Objednateli doručeno oznámení o nemožnosti doručit e-mailovou zprávu obsahující požadavek.

2.4 Podpora spočívající v odstraňování vad podle odst. 2.1 písm. d) Smlouvy bude poskytována na základě požadavků Objednatele zadaných prostřednictvím hot-line. Vadou SW se rozumí rozpor mezi skutečnými vlastnostmi SW a vlastnostmi specifikovanými v dokumentaci vztahující se k SW.

Požadavek zadává Objednatel telefonicky nebo písemně na uvedenou e-mailovou adresu helpdesku dle odst. 12.1 písm. f) Smlouvy. V případě zadání požadavku telefonicky je Objednatel povinen jej zaslat Dodavateli také písemně.

2.5 Požadavek dle předchozího odstavce Smlouvy musí obsahovat alespoň tyto údaje:

a) jméno osoby, která vadu nahlásila;

b) jméno odpovědné osoby ze strany Objednatele;

c) kategorií vady a očekávaný termín vyřešení;

d) popis vady včetně simulace v testovacím prostředí.

Každá vada bude hlášena samostatným požadavkem.

2.6 Kategorie vad:

Kategorie	Definice
A	Standardní provozní procesy jsou vážně ovlivněny a nezbytné úlohy nemohou být plněny. Některé nebo všechny systémy podporující hlavní provozní procesy selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna informační podpora činnosti objednatele.
B	Jsou dotčeny provozní procesy v míře způsobující ztěžování výkonu konkrétní činnosti. Podporované činnosti jsou výrazně ovlivněny z důvodu selhání nebo omezení některé ze systémových funkcí podporující důležité procesy. V případě současného výskytu více vad kategorie B může nastat situace, kdy vzájemné působení těchto vad způsobí kumulaci negativního dopadu na provozní procesy, pak budou i jednotlivé vady způsobující tuto kumulaci hodnoceny kategorií A.
C	Stav služby, kdy nejsou ohroženy hlavní funkce systému/aplikace. Po dobu výpadku lze nahradit nefunkční část náhradním řešením.

2.7 Požadované garance:

Kategorie	Reakční doba	Doba vyřešení
A	1 hodina	NBD
B	4 hodiny	NBD+1
C	NBD	NBD+5

NBD (Next Business Day) – následující pracovní den

NBD+x (Next Business Day + x BD) – x-tý pracovní den po NBD

Tyto doby platí v časovém období dle odst. 2.2 této Smlouvy, nedohodnou-li se Smluvní strany v souladu s odst. 2.8 na době delší. Reakční dobou se rozumí potvrzení Dodavatele o přijetí požadavku učiněné telefonicky a následně vždy písemně e-mailem na kontakty Objednatele uvedené odst. 12.1 této Smlouvy. Následně Dodavatel zašle návrh způsobu řešení a zahájí práce na odstranění vady.

2.8 Na termínu odstranění vady se Smluvní strany dohodnou písemně prostřednictvím odpovědných osob ve věcech technických. O odstranění vady následně Smluvní strany vyhotoví oboustranně podepsaný zápis – akceptační protokol.

2.9 Bylo-li Objednatelem umožněno poskytování Podpory prostřednictvím vzdáleného přístupu, bude vada primárně odstraněna prostřednictvím vzdáleného přístupu. V ostatních případech nebo není-li Dodavatel schopen vadu prostřednictvím vzdáleného přístupu odstranit, garantuje Dodavatel příjezd konzultanta Dodavatele na místo podle určení Objednatele za účelem poskytnutí Podpory.

3 Cena Plnění a platební podmínky

3.1 Ceny jednotlivých složek Plnění jsou uvedeny v Příloze č. 2 Smlouvy.

3.2 Daňový doklad na cenu Plnění dle odst. 1.2 písm. a) Smlouvy bude vystaven Dodavatelem po řádném poskytnutí příslušného Plnění bez vad v souladu se Smlouvou. Nedílnou součástí tohoto daňového dokladu bude Objednatelem potvrzený Akceptační protokol dle čl. 5 této Smlouvy. Dnem uskutečnění zdanitelného plnění je den podpisu Akceptačního protokolu Objednatelem.

3.3 Cena Podpory dle odst. 1.2 písm. b) Smlouvy poskytnuté v příslušném kalendářním měsíci bude Objednatelem hrazena měsíčně předem. Dodavatel vystaví daňový doklad k tomuto Plnění vždy první den příslušného období poskytování Podpory (kalendářního měsíce); tento den se zároveň považuje za den uskutečnění zdanitelného plnění.

3.4 Pokud bude Podpora poskytována jen po část kalendářního měsíce, hradí se za příslušný kalendářní měsíc poměrná část měsíční ceny Podpory. V případě, že dojde k ukončení Smlouvy před uplynutím období, za které byla Objednatelem uhrazena cena za Podporu předem, je Dodavatel povinen nejdéle do 10 kalendářních dnů od data ukončení Smlouvy vystavit a zaslat Objednateli opravný daňový doklad na částku uhrazené Podpory, kterou Objednatel nespotřeboval, a tuto částku zaslat na účet Objednatele uvedený v záhlaví této Smlouvy.

3.5 Cena Plnění zahrnuje veškeré náklady Dodavatele spojené s řádným a úplným plněním Smlouvy a poskytnutím Plnění Objednateli, včetně těch, které ve Smlouvě výslovně uvedeny nejsou, ale Dodavatel jakožto odborník a osoba poskytující Plnění s odbornou péčí podle Smlouvy o nich ke dni nabytí účinnosti Smlouvy při vynaložení úsilí, které lze spravedlivě požadovat, vědět měl nebo mohl vědět, že jsou k poskytnutí řádného Plnění nezbytné.

3.6 Splatnost daňového dokladu vystaveného Dodavatelem je třicet (30) kalendářních dnů ode dne jeho vystavení Dodavatelem.

3.7 Objednatel neposkytuje Dodavateli jakékoliv zálohy na cenu.

3.8 Daňové doklady zasílá Dodavatel Objednateli postupem dle odst. 2.6 VOP.

4 Doba, místo Plnění

4.1 Plnění dle odst. 1.2 písm. a) Smlouvy bude řádně poskytnuto nejpozději do 31.12.2025.

4.2 Poskytování Podpory dle odst. 1.2 písm. b) Smlouvy bude zahájeno ode dne poskytnutí Licencí dle odst. 1.2 písm. a) Smlouvy, ne však dříve, než 1.1.2026. Podpora bude poskytována po dobu 48 měsíců.

4.3 Místem plnění je: Česká pošta, s.p., Olšanská 38, 130 00 Praha 3, není-li nestanoví-li jinak Objednatel v požadavku na Podporu dle odst. 2.4 Smlouvy. Podpora může poskytována i prostřednictvím vzdáleného přístupu.

5 Kontrola a akceptace SW

5.1 Řádným poskytnutím Plnění dle čl. 1.2 písm. a) Smlouvy se rozumí implementace požadovaného SW do infrastruktury Objednatele tak, aby Objednatel mohl zahájit využívání SW.

5.2 Spolu s Plněním dle odst. 1.2 písm. a) Smlouvy bude předána také veškerá dokumentace (produktová, uživatelská) vztahující se k SW, bez níž by nemohlo docházet k řádnému užívání tohoto Plnění. Dokumentace bude předána v elektronické podobě, v českém jazyce.

5.3 Kontrola a akceptace Plnění dle odst. 1.2 písm. a) Smlouvy probíhá na základě testování pracovníky Objednatele a je potvrzena podpisem akceptačního protokolu (dále jen „**Akceptační protokol**"), jehož vzor je Přílohou č. 4 Smlouvy, a to následujícím způsobem:

a) Dodavatel zpracuje návrh Akceptačního protokolu a předkládá jej Objednateli. Předání a akceptace Objednatelem bude potvrzena podpisem zástupce Objednatele ve věcech technických dle odst. 12.1 písm. d) Smlouvy na Akceptačním protokolu.

b) Objednatel akceptaci Plnění odmítne v případě, že Plnění vykazuje natolik vážné vady, že nemůže sloužit svému účelu vůbec nebo s výraznými omezeními. V případě méně vážných vad může Objednatel akceptaci Plnění odmítnout nebo Plnění akceptovat s výhradami. Neodmítnutí převzetí Plnění však nezbavuje Objednatele jeho nároků z odpovědnosti Dodavatele za vady.

c) V případě, že předání nebo akceptace byla provedena s výhradami Objednatele, je Dodavatel povinen zjednat nápravu do pěti (5) kalendářních dnů, nebude-li dohodou Smluvních stran stanoveno jinak.

d) Bylo-li Plnění předáno a akceptováno, je Dodavatel oprávněn vystavit daňový doklad na cenu dle odst. 3.2 Smlouvy. Bylo-li Plnění předáno nebo akceptováno s výhradou, Dodavateli vznikne právo na zaplacení ceny a vystavení daňového dokladu až po zjednání nápravy a bezvýhradné akceptaci Plnění.

6 Práva a povinnosti smluvních stran

6.1 Plnění musí být poskytnuto bez jakýchkoli vad, ať již faktických či právních, v souladu s veškerými právními předpisy, technickými požadavky a technickými a bezpečnostními normami, které se na Plnění vztahují, a to jak normami závaznými, tak doporučujícími.

6.2 V rámci realizace předmětu Smlouvy má každá Smluvní strana zejména následující povinnosti:

a) vzájemně spolupracovat a poskytovat druhé Smluvní straně veškeré informace potřebné pro řádné plnění svých povinností vyplývajících ze Smlouvy;

b) poskytovat druhé Smluvní straně úplné, pravdivé a včasné informace o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění dle Smlouvy;

c) plnit své povinnosti vyplývající ze Smlouvy tak, aby nedocházelo k prodlení s plněním povinností vázaných k jednotlivým termínům.

6.3 Objednatel se zavazuje v termínech stanovených touto Smlouvou, jinak v termínech odpovídajících postupu realizace Plnění, poskytnout Dodavateli potřebnou součinnost v následujícím rozsahu:

a) poskytovat Dodavateli potřebné dokumenty a informace, je-li povinnost k jejich poskytnutí uvedena ve Smlouvě (včetně příloh), nebo bylo-li tak dohodnuto v rámci jednání Smluvních stran;

b) umožnit pracovníkům Dodavatele uvedeným v písemném seznamu dle odst. 7.4 Smlouvy předloženém Dodavatelem v předem dohodnutém termínu přístup na pracoviště Objednatele, je-li to nezbytné pro realizaci předmětu Smlouvy, a umožnit Dodavateli vzdálený přístup do informačních systémů Objednatele, je-li to pro realizaci předmětu Smlouvy nezbytné;

c) seznámit Dodavatele s interními pravidly a předpisy Objednatele v oblasti bezpečnosti ICT systémů a BOZP, které bude Dodavatel povinen dodržovat;

d) dle potřeby a řešeného tématu zajistit účast a součinnost odpovědných pracovníků Objednatele při schvalování, analýzách, testování, akceptaci, seminářích, školeních apod.;

e) poskytovat informace o ostatních projektech v daném prostředí, pokud budou mít jakýkoli vliv na plnění povinností Dodavatele z této Smlouvy;

f) zajistit součinnost třetích stran, které nejsou v přímém smluvním vztahu s Dodavatelem, avšak jejichž činnost se přímo i nepřímo může dotýkat plnění dle této Smlouvy, pokud bude tato součinnost nezbytná pro plnění povinností Dodavatele;

g) zajistit datovou a internetovou konektivitu, tj. komunikační kanál poskytující připojení k dílčím systémům Objednatele.

6.4 Dodavatel se v souvislosti s realizací předmětu této Smlouvy zavazuje zejména:

a) poskytovat Plnění v souladu se Smlouvou, řádně a včas, s řádnou a odbornou péčí a potřebnými odbornými schopnostmi pro poskytování Plnění tak, aby bylo dosaženo účelu Smlouvy;

b) poskytovat Plnění v souladu s obecně závaznými právními předpisy a pokyny Objednatele, pokud tyto nejsou v rozporu s těmito normami nebo zájmy Objednatele. Dodavatel je povinen při výkonu své činnosti včas písemně upozornit Objednatele na zřejmou nevhodnost jeho pokynů, jejichž následkem může vzniknout újma nebo nesoulad s obecně závaznými právními předpisy. Pokud Objednatel navzdory tomuto upozornění trvá na svých pokynech, Dodavatel neodpovídá za jakoukoli újmu vzniklou v této příčinné souvislosti;

c) při plnění předmětu této Smlouvy brát na zřetel provozní potřeby Objednatele, postupovat podle pravidel obvyklých pro zpracování dat a v úzké součinnosti s Objednatelem provádět jednotlivá dílčí Plnění;

d) pokud v průběhu plnění povinností dle Smlouvy vznikne na straně Dodavatele potřeba využít služeb třetí strany – poddodavatele, učinit tak jen po předchozím souhlasu Objednatele a jen tehdy, pokud bude nový poddodavatel splňovat potřebnou kvalifikaci. V případě, že Objednatel souhlas k využití poddodavatele neudělí, není Dodavatel oprávněn takovou poddodávku udělit. V případě souhlasu Objednatele a následného využití služeb třetí strany bude Dodavatel odpovídat za třetí stranu, jako by plnil sám, včetně odpovědnosti za způsobenou újmu. Dodavatel je povinen zajistit, aby jeho poddodavatel poskytoval plnění v souladu s touto Smlouvou a dodržoval veškerá ujednání mezi Smluvními stranami;

e) informovat bezodkladně Objednatele o jakýchkoliv zjištěných překážkách Plnění, byť by za ně Dodavatel neodpovídal a o uplatněných nárocích třetích osob, které by mohly Plnění ovlivnit;

f) dbát, aby nebyla poškozena dobrá obchodní pověst a dobré jméno Objednatele. Při poskytování plnění musí Dodavatel vždy sledovat zájmy Objednatele;

g) činit všechna potřebná opatření k tomu, aby jeho činností nedošlo ke škodám na majetku Objednatele, jeho zaměstnanců nebo třetích stran, anebo k poškození zdraví zaměstnanců Objednatele nebo třetích osob, jimž by Objednatel za takto způsobenou újmu odpovídal;

h) odčinit majetkovou i nemajetkovou újmu vzniklou Objednateli činností, nečinností nebo opomenutím Dodavatele;

i) pro poskytování Plnění neužívat zaměstnance Objednatele, ani s nimi v této souvislosti neuzavírat jakýkoliv právní vztah s výjimkou potřebné a přiměřené součinnosti, není-li v této Smlouvě stanoveno jinak;

j) na vyžádání Objednatele se zúčastnit osobní schůzky, pokud Objednatel požádá o schůzku nejpozději dva (2) pracovní dny předem. V mimořádně naléhavých případech je možno tento termín po dohodě obou Smluvních stran zkrátit;

k) dodržovat veškerá interní pravidla a předpisy Objednatele týkající se bezpečnosti ICT systémů, BOZP a požární ochrany, byl-li s nimi Objednatelem seznámen, a účastnit se na výzvu Objednatele školení v oblasti bezpečnosti ICT systémů, pravidel BOZP a požární ochrany Objednatele;

l) plnit v kvalitě potřebné pro dosažení parametrů stanovených Smlouvou a odpovídat za to, že případné vady Plnění poskytnutého dle Smlouvy řádně odstraní, případně nahradí plněním bezvadným v souladu se Smlouvou;

m) umožnit Objednateli kontrolovat, zda Dodavatel poskytuje Plnění řádně;

n) mít po celou dobu trvání Smlouvy sjednáno pojištění odpovědnosti za majetkové i nemajetkové újmy způsobené v souvislosti s plněním Smlouvy Dodavatelem nebo osobou, za niž odpovídá, s pojistnou částkou nejméně 10 000 000 Kč (slovy: deset milionů korun českých). Při vzniku pojistné události zabezpečuje ihned po jejím vzniku veškeré úkony vůči pojistiteli Dodavatel. Objednatel je povinen poskytnout v souvislosti s pojistnou událostí Dodavatele veškerou součinnost, která je v jeho možnostech. Dodavatel je povinen doložit Objednateli na výzvu doklad o uzavření pojištění a úhradě pojistného dle tohoto odstavce do 5 pracovních dnů od obdržení výzvy. Pro vyloučení pochybností se uvádí, že ustanovení odst. 7.1 VOP se pro potřeby plnění této Smlouvy nepoužije;

7 Realizační tým

7.1 Dodavatel je povinen za účelem poskytování Plnění zajistit dostatečnou kapacitu svých pracovníků s odpovídající kvalifikací a zkušenostmi.

7.2 Dodavatel je povinen za účelem poskytování Plnění ustavit členy realizačního týmu pro realizaci této Smlouvy a určit jejich pravomoci (dále jen „**Realizační tým**“). Složení Realizačního týmu Dodavatel sdělí před zahájením plnění Objednateli, přičemž členy Realizačního týmu musí být osoby, kterými Dodavatel prokázal technickou kvalifikaci v rámci Zadávacího řízení v odpovídajících pozicích. Dodavatel zajistí kontinuitu členů Realizačního týmu v průběhu trvání Smlouvy. Bude-li ze závažných důvodů (např. ukončení pracovněprávního či jiného smluvního vztahu, úmrtí, dlouhodobá pracovní neschopnost) nutné nahradit člena Realizačního týmu, kterým Dodavatel prokázal technickou kvalifikaci v rámci Zadávacího řízení, musí mít nový člen Realizačního týmu stejnou nebo vyšší kvalifikaci, než jakou disponoval dosavadní člen Realizačního týmu na dané pozici. Změna v Realizačním týmu bude neprodleně oznámena Objednateli.

7.3 Jednotlivé činnosti prováděné v rámci Plnění nespadající do činností členů Realizačního týmu mohou být prováděny i jinými osobami než členy Realizačního týmu.

7.4 Dodavatel je povinen předložit Objednateli před zahájením Plnění seznam pracovníků, pro které bude požadovat přístup na pracoviště Objednatele a vzdálený přístup do informačního systému Objednatele, je-li to pro plnění Smlouvy nezbytné.

8 Práva duševního vlastnictví

8.1 Podmínky užití Licence se řídí licenčními podmínkami výrobce SW uvedenými v Příloze č. 3 Smlouvy (dále jen „**Licenční ujednání**“). Smluvní strany výslovně sjednávají, že Dodavatel je povinen zajistit Objednateli oprávnění k výkonu práva užít SW a jakékoli aktualizace (update), nové verze (upgrade), opravy či úpravy SW dodané v rámci poskytování Plnění tak, aby mohl být naplněn účel Smlouvy. Pro vyloučení pochybností se uvádí, že odst. 8.3 VOP a 8.5 VOP pro dodávky zboží Objednatele se pro potřeby plnění této Smlouvy nepoužijí.

8.2 Dodavatel prohlašuje, že je oprávněn Plnění v rozsahu sjednaném v této Smlouvě Objednateli poskytnout, že uzavřením a plněním této Smlouvy neporušuje žádná práva duševního vlastnictví, ani jiná práva třetích osob. Dodavatel odpovídá za to, že Objednatel užíváním SW v rozsahu poskytnuté Licence neporušuje žádná práva třetích osob. Dodavatel je povinen umožnit Objednateli nerušené užívání SW v rozsahu udělené Licence a chránit jej, ať sám nebo prostřednictvím výrobce SW, před nároky třetích osob vznesenými vůči Objednateli v souvislosti s užíváním SW.

8.3 Objednatel není povinen žádnou z licencí nabytých na základě této Smlouvy využít.

9 Práva z vadného plnění, záruka za jakost

9.1 Plnění má vady, jestliže nebylo poskytnuto tak, jak bylo sjednáno nebo poruší-li Dodavatel svou povinnost v souvislosti s poskytováním Plnění. Za vady se považují i vady v dokladech a dokumentech dodaných spolu s předmětem Plnění a právní vady.

9.2 U služeb prováděných Dodavatelem v rámci Podpory poskytuje Dodavatel Objednateli záruku na jakost výstupů v délce **dvacet čtyři (24) měsíců** ode dne poskytnutí těchto služeb v rámci Podpory. Dodavatel však neodpovídá za vady výstupů, pokud byly způsobeny zásahem do takových výstupů ze strany Objednatele nebo jím pověřené osoby; na takové zásahy bude Dodavatel předem upozorněn. Objednatel je povinen vady výstupů Podpory písemně oznámit Dodavateli prostřednictvím e-mailu odpovědnými osobami Objednatele na adresu odpovědných osob Dodavatele do patnácti (15) dnů ode dne jejich zjištění. Dodavatel v takovémto případě prošetří oznámenou vadu a v případě, že se na ni vztahuje záruka dle této Smlouvy, vadu Podpory odstraní ve lhůtě 48 hodin od nahlášení vady. Objednatel mu přitom poskytne potřebnou součinnost, a to zejména pro odhalení příčiny vady. V případě opakovaného prodlení s odstraněním vady ve lhůtě dle předchozí věty je Objednatel oprávněn odstoupit od Smlouvy. Odst. 5.2 a 5.3 VOP se v tomto případě nepoužije.

10 Bezpečnost ICT systémů

10.1 Objednatel zastává pozici pověřené osoby ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „ZKB“) a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „VKB“) a je správcem kritické informační infrastruktury (dále jen „KII“). Předmět plnění bude součástí KII Objednatele, a proto jsou již v rámci této smlouvy na něj kladeny požadavky dle Zákona o kybernetické bezpečnosti a **Dodavatel je touto Smlouvou jmenován významným dodavatelem**.

10.2 Dodavatel se zavazuje dodržovat požadavky na bezpečnost ICT, které vyplývají z ZKB, VKB, GDPR, ISO rodiny 27000 a případně požadavky vyplývající z bezpečnostního standardu PCI DSS, a které jsou podrobně vymezeny v Příloze č. 7 Smlouvy.

11 Nemožnost plnění

11.1 Jestliže vznikne na straně Dodavatele nemožnost plnění dle § 2006 a § 2007 Občanského zákoníku, Dodavatel písemně uvědomí bez zbytečného odkladu, nejpozději však do pěti (5) kalendářních dnů od jejího vzniku, o této skutečnosti a její příčině Objednatele. Pokud není jinak stanoveno písemně Objednatelem, bude Dodavatel pokračovat v realizaci svých povinností 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 devadesát (90) kalendářních dní, je Objednatel oprávněn od Smlouvy odstoupit.

11.2 Ustanovení tohoto odstavce Smlouvy nezbavuje žádnou ze Smluvních stran její povinnosti k úhradě plateb v té době již splatných.

12 Kontaktní osoby

12.1 Kontaktní osoby Objednatele a Dodavatele **ve věcech obchodních** pro účely této Smlouvy jsou:

a) **Za Objednatele:**

[redacted]

b) **Za Dodavatele:**

[redacted]

[redacted]

Kontaktní osoby Objednatele a Dodavatele **ve věcech technických** pro účely této Smlouvy jsou:

c) **Za Objednatele:**

[redacted]

Kontaktní osoby Objednatele pověřené podáváním a přijímáním případů Podpory:

[redacted]

d) **Kontaktní osoba za Dodavatele:**

[redacted]

e) **Helpdesk Dodavatele:**

Helpdesk

[redacted]

www: monetplus.cz

12.2 Pouze kontaktní osoby Objednatele a Dodavatele jsou oprávněni vznášet vůči druhé Smluvní straně požadavky související s plněním této Smlouvy. Smluvní strany se zavazují v průběhu plnění Smlouvy nezměnit kontaktní osoby bez závažných důvodů. V případě změny kontaktní osoby je Smluvní strana povinna neprodleně o této skutečnosti písemně informovat druhou Smluvní stranu.

13 Smluvní pokuty, odpovědnost za újmu

13.1 Smluvní strany dohodly odlišně od ustanovení odst. 11.1 písm. a) VOP, že v případě prodlení Objednatele s dodržením lhůty stanovené v odst. 4.1 Smlouvy je Objednatel oprávněn požadovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 2 000,- Kč (slovy: dva tisíce korun českých) za každý započatý den prodlení.

13.2 Smluvní strany dohodly odlišně od ustanovení odst. 11.1 písm. a) VOP, že v případě prodlení Objednatele s dodržením lhůty stanovené v odst. 4.2 Smlouvy je Objednatel oprávněn požadovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 1 000,- Kč (slovy: jeden tisíc korun českých) za každý započatý den prodlení.

13.3 Smluvní strany dohodly odlišně od ustanovení odst. 11.1 písm. b) VOP, že v případě prodlení s odstraněním záručních vad Plnění je Objednatel oprávněn požadovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 1 000,- Kč (slovy: jeden tisíc korun českých), a to za každou započatou hodinu prodlení a každou vadu.

13.4 V případě ztráty či poškození, pozměnění či zneužití dat Objednatele je Objednatel oprávněn požadovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 500 000,- Kč (slovy: pět set tisíc korun českých) za každý jednotlivý případ.

13.5 V případě porušení kterékoli z povinností Dodavatele dle čl. 10 Smlouvy je Objednatel oprávněn požadovat od Dodavatele zaplacení smluvní pokuty ve výši 100 000,- Kč (slovy: sto tisíc korun českých) za každý případ porušení.

13.6 Smluvní strany dohodly odlišně od ustanovení odst. 11.1 písm. f) VOP, že v případě nesplnění povinnosti Dodavatele doložit sjednání pojištění a úhrady pojistného ve lhůtě dle odst. 6.4 písm. o) Smlouvy je Objednatel oprávněn požadovat od Dodavatele zaplacení smluvní pokuty ve výši 10 000 Kč (slovy: deset tisíc korun českých) za každý případ porušení.

13.7 Smluvní strany dohodly odlišně od ustanovení odst. 11.1 písm. d) VOP, že za každé jednotlivé porušení povinnosti, týkající se ochrany Obchodního tajemství a Důvěrných informací dle odst. 10.1 VOP nebo čl. 8 Smlouvy ze strany Dodavatele, je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých).

13.8 Smluvní strany dohodly odlišně od ustanovení odst. 11.1 písm. e) VOP, že v případě, že se kterékoli prohlášení Dodavatele dle odst. 9.1 VOP ukáže, byť jen z části, jako nepravdivé, je Dodavatel povinen

uhradit Objednateli smluvní pokutu ve výši 100 000,- Kč (slovy: sto tisíc korun českých) za každý případ, kdy se kterékoli prohlášení ukázalo, byť jen zčásti, jako nepravdivé.

13.9 Smluvní strany dohodly odlišně od ustanovení odst. 11.1 písm. c) VOP, že v případě, že dojde k porušení povinnosti Dodavatele, jež zakládá nárok Objednatele na odstoupení od Smlouvy, je Objednatel oprávněn bez ohledu na skutečnost, zda využije svého práva na odstoupení od Smlouvy, účtovat Dodavateli smluvní pokutu ve výši 250 000,- Kč (slovy: dvě stě padesát tisíc korun českých) za každý případ porušení takové povinnosti. Tím není dotčeno právo na vymáhání způsobené újmy.

13.10 V případě neposkytnutí řádné součinnosti dle odst. 14.4 Smlouvy je Objednatel oprávněn požadovat a Dodavatel povinen zaplatit smluvní pokutu ve výši 100 000,- Kč (slovy: sto tisíc korun českých) za každý jednotlivý případ.

14 Doba trvání Smlouvy

14.1 Tato Smlouva nabývá platnosti dnem jejího podpisu Smluvními stranami a účinnosti dnem uveřejnění v registru smluv podle zákona o registru smluv. Plnění předmětu této Smlouvy v době od platnosti Smlouvy do její účinnosti se považuje za plnění podle této Smlouvy a práva a povinnosti z něj vzniklé se řídí touto Smlouvou.

14.2 Tato Smlouva se uzavírá na dobu určitou, a to na dobu 48 měsíců ode dne zahájení poskytování Podpory ve smyslu odst. 4.2 Smlouvy.

14.3 Účinnost této Smlouvy lze ukončit předčasně před sjednanou dobou trvání výhradně ze zákonných důvodů, písemnou dohodou Smluvních stran, výpovědí nebo odstoupením z důvodů uvedených v zákoně nebo v této Smlouvě.

14.4 V případě zániku smluvního závazkového vztahu založeného Smlouvou je Dodavatel povinen poskytnout Objednateli nebo Objednatelem určené třetí osobě nezbytnou součinnost za účelem zajištění řádného exportu dat Objednatele do jiného úložiště dat tak, aby Objednateli nevznikla újma, přičemž Dodavatel se zavazuje tuto součinnost poskytovat s odbornou péčí, zodpovědně, a to do doby zániku smluvního závazkového vztahu založeného Smlouvou. Dodavatel je povinen v rámci součinnosti dle předchozí věty poskytnout Objednateli nebo jím určeným třetím osobám informace potřebné k převedení činností dle této Smlouvy novému Dodavateli Služeb či novému Dodavateli služeb podobných službám či s nimi jinak spojených. Úhrada nákladů spojených s poskytnutím součinnosti dle tohoto odstavce je zahrnuta v ceně dle čl. 3 Smlouvy.

14.5 Po ukončení Smlouvy zůstává zachována platnost a účinnost ustanovení Smlouvy, týkající se odpovědnosti za vady, záruky za jakost, licenčních ujednání, ochrany Důvěrných informací, ochrany Osobních údajů, smluvních pokut, náhrady újmy a jiných ze své povahy přetrvávajících nároků či závazků.

15 Závěrečná ustanovení

15.1 Tato Smlouva nabývá platnosti dnem jejího podpisu Smluvními stranami a účinnosti dnem zveřejnění v registru smluv podle zákona o registru smluv. Plnění předmětu této Smlouvy v době od platnosti Smlouvy do její účinnosti se považuje za plnění podle této Smlouvy a práva a povinnosti z něj vzniklé se řídí touto Smlouvou.

15.2 Pro případ, že tato Smlouva není uzavírána za přítomnosti obou Smluvních stran, platí, že Smlouva nebude uzavřena, pokud ji Prodávající podepíše s jakoukoliv změnou či odchylkou, byť nepodstatnou, nebo dodatkem. To platí i v případě připojení obchodních podmínek Prodávajícího, které budou odporovat svým obsahem jakýmkoliv způsobem textu této Smlouvy, případně VOP.

15.3 Smluvní strany výslovně potvrzují, že si vzájemně sdělily veškeré okolnosti důležité pro uzavření Smlouvy. Smluvní strany prohlašují, že se dohodly o veškerých náležitostech Smlouvy.

15.4 Je-li Smlouva vyhotovena v listinné podobě, je vyhotovena ve dvou (2) stejnopisech s platností originálu, z nichž každá ze Smluvních stran obdrží po jednom (1) stejnopisu. Pokud je Smlouva vyhotovena v elektronické podobě, obě Smluvní strany obdrží elektronický originál opatřený elektronickými podpisy obou Smluvních stran, včetně časového razítka dle příslušných právních předpisů.

15.5 Nedílnou součástí této Smlouvy jsou následující Přílohy:

Příloha č. 1 - Specifikace SW

Příloha č. 2 - Cena

Příloha č. 3 - Licenční ujednání

Příloha č. 4 - Vzor akceptačního protokolu

Příloha č. 5 - Všeobecné obchodní podmínky pro poskytování služeb a Všeobecné obchodní podmínky pro dodávky zboží Objednatele

Příloha č. 6 - Požadované technické parametry

Příloha č. 7 – Požadavky na bezpečnost ICT – Pravidla pro dodavatele

NA DŮKAZ TOHO, že Smluvní strany s obsahem Smlouvy souhlasí, rozumí ji a zavazují se k jejímu plnění, připojují své podpisy a prohlašují, že tato Smlouva byla uzavřena podle jejich svobodné a vážné vůle prosté tísně, zejména tísně finanční.

V Praze

Mgr. Vlastimil Halla, MBA
ředitel úseku generálního ředitele
Česká pošta, s.p.

Ve Zlíně

Ing. Břetislav Endrys
předseda představenstva
MONET+,a.s.

Ing. Jan Vavrys
člen představenstva
MONET+,a.s.

Příloha č. 1 – Specifikace SW

Předmětem plnění je **dodávka SW pro zajištění služeb certifikační autority PostSignum** pro služby provozované Objednatelem v roli kvalifikovaného poskytovatele služeb vytvářejících důvěru. SW nahradí doposud používaný SW UNICERT od společnosti Verizon.

Předmět plnění bude dodán v souladu s licenčními podmínkami nejenom jako celku, ale i v souladu s licenčními podmínkami jednotlivých komponent. Dodavatel dodá k SW třetích stran (pokud byl použit) příslušné licenční oprávnění, tak aby Objednatel provozoval dodané SW řešení v souladu se všemi licenčními podmínkami. Dodavatel bere na vědomí, že Objednatel má vlastní infrastrukturu IT s licenčním portfoliem, které podléhá nebo může podléhat smluvním závazkům s vendorem k celopodnikovému pokrytí. Dodavatel v rámci řešení bude v případě dodávky SW licencí třetí strany respektovat platné celopodnikové smluvní závazky Objednatele s dodavateli licenčních produktů a podpory.

1. **Výhled provozovaných CA s predikcí počtu vydaných certifikátů za období provozu 10 let**

- Root RSA 1 (500 certifikátů)
  a. SubCA RSA QCA – kvalifikované certifikáty pro podpis a pečeť (10 mil. certifikátů)
  b. SubCA RSA VCA – komerční osobní a serverové certifikáty (5 mil. certifikátů)
- Root ECC 11 (500 certifikátů)
  c. SubCA ECC QCA – kvalifikované certifikáty pro podpis a pečeť (10 mil. certifikátů)
  d. SubCA ECC VCA – komerční osobní a serverové certifikáty (5 mil. certifikátů)
- Root ECC 21 (500 certifikátů)
  e. SubCA ECC TSA – kvalifikované certifikáty pro TSA (1000 certifikátů)
- Root ECC 31 (500 certifikátů)
  f. SubCA ECC QWAC – kvalifikované certifikáty pro TLS dle eIDAS (1 mil. certifikátů)
- Root ECC 41 (500 certifikátů)
  g. SubCA ECC TLS – komerční certifikáty pro TLS (1 mil. certifikátů)

Parametry pro Root CA:

- Délka platnosti – 15 let
- Provoz offline na fyzickém serveru s vloženou PCI HSM kartou s podporou RSA, RSA-PSS, ECC
- Všechny Root CA budou umístěné na jednom serveru s jedním Security Worldem

Parametry pro podřízené CA:

- Délka platnosti – 10 let
- Provoz na fyzickém/virtuálním serveru s klíči uloženými na síťovém HSM s podporou RSA, RSA-PSS, ECC
- Provoz podřízené CA je plánovaný min. na dvou serverech pro kvalifikované/komerční podřízené CA.
- Všechny podřízené CA budou mít sdílený Security World

Poznámka: Počet všech výše uvedených CA se může zdvojnásobit, a to v případě vybudování navazující CA. V tomto případě se původní CA stává jen pasivní pro účely zneplatňování platných certifikátů, tzn. při platnosti certifikátů 3 roky by souběžný provoz CA trval max. 3 roky.

2. **Požadované technické parametry**

Požadované technické parametry jsou uvedené v samostatné tabulce (v příloze č. 6).

Příloha č. 2 – Cena

Plnění	popis Plnění	Kč bez DPH
SW (licence) a implementace dle odst. 1.2 a) Smlouvy	Předmětem je dodávka SW licencí a implementace v souladu s přílohou č. 1 a přílohou č. 6 Smlouvy. SW licence - Certifikační autorita Certificate generation service, CRL assembling service, OCSP, WWW RA, PKI API, Event collector, Smartcard Logon Standalone	12 750 000,00

Plnění	počet měsíců	Kč bez DPH za	
		1 měsíc	uvedený počet měsíců
Podpora SW dle odst. 1.2 b) Smlouvy	48	215 000,00	10 320 000,00

Celková cena Plnění	**23 070 000,00**

Příloha č. 3 Smlouvy: Licenční ujednání

Objednatel bude SW využívat pro zajištění služeb pro interní potřebu i pro komerční využití pro své zákazníky. Poskytování služeb pro zákazníky bude zpoplatněno. Nad rámec této dodávky SW nemůže dodavatel ani třetí strana požadovat jakýkoliv poplatek za poskytování služeb prostřednictvím tohoto SW, např. poplatek za komerční licenci pro poskytování certifikátů třetím stranám.

Uvádíme, že licenční ujednání níže je určeno koncovým uživatelům (v tomto případě zákazníkům Objednatele), přičemž pro samotného Objednatele (Českou poštu a.s.) platí v úplném rozsahu podmínky uvedené ve vzoru smlouvy (včetně všeobecných obchodních podmínek).
Licence jsou Objednateli uděleny jako nevýhradní, volně převoditelné, místně a časově neomezené, ve specifikovaném množství, včetně oprávnění udělovat ve stejném rozsahu podlicence.

LICENČNÍ UJEDNÁNÍ PRO POUŽÍVÁNÍ SOFTWARE SPOLEČNOSTI MONET+, a.s.

DŮLEŽITÉ! ČTĚTE POZORNĚ: Toto licenční ujednání („EULA“) upravuje podmínky, za kterých koncový uživatel může používat získané softwarové produkty společnosti MONET+, a.s. (dále jen MONET+), včetně příslušných instalačních médií, tištěných materiálů, dokumentace.

Tyto podmínky se vztahují pouze na řádně (legálně) získaný software společnosti MONET+.

Instalací, kopírováním nebo jakýmkoliv jiným užitím software společnosti MONET+ výslovně potvrzujete, že souhlasíte se všemi licenčními podmínkami tohoto ujednání.

Důrazně proto doporučujeme se s těmito licenčními podmínkami seznámit před instalací software společnosti MONET+.

Pokud s těmito podmínkami nesouhlasíte, nesmíte software společnosti MONET+ používat žádným způsobem a s případně již obdrženým (získaným) produktem se obraťte na svého dodavatele (poskytovatele).

PŘEDMĚT LICENČNÍHO UJEDNÁNÍ

Předmětem tohoto licenčního ujednání je softwarový produkt:

- **Certifikační autorita - Certificate generation service**
- **CRL assembling service**
- **OCSP**
- **WWW RA**
- **PKI API**
- **Event collector**
- **Smartcard Logon Standalone**

(dále také softwarový produkt nebo software) společnosti MONET+.

Termín software zahrnuje i veškeré vyšší či modifikované verze, aktualizace, dodatky a kopie produktu.

LICENCE NA SOFTWAROVÝ PRODUKT

Společnost MONET+ Vám uděluje v souvislosti se získáním softwarového produktu pouze níže specifikovaná práva za předpokladu, že budete striktně dodržovat veškeré podmínky těchto licenčních podmínek takto:

1. INSTALACE A POUŽITÍ

Můžete instalovat a užívat daný počet řádně zakoupených instalací software. Spuštění a užívání software je striktně a neoddělitelně vázáno ke každé licenci. Tato licence nesmí být sdílena.

2. ZÁLOŽNÍ KOPIE

Nesmíte vytvářet žádné jiné kopie softwaru ani tištěných materiálů dodaných se softwarem. Originální disk, digitální nosič ani jeho záložní kopii nesmíte zapůjčit, pronajmout, poskytnout na leasing ani žádným jiným způsobem převést třetí osobě.

3. VÝHRADA PRÁV A VLASTNICTVÍ

Společnost MONET+ si výslovně vyhrazuje všechna autorská práva, která nejsou výslovně uvedena v tomto licenčním ujednání.

Tento produkt společnosti MONET+ je chráněn autorským zákonem a dalšími zákony a mezinárodními dohodami o duševním vlastnictví.

Společnost MONET+ vykonává veškerá osobnostní i majetková autorská práva, která se žádným způsobem nepřevádí, k software se pouze uděluje oprávnění k jeho užití.

4. ZÁKAZ REVERZNÍHO INŽENÝRSTVÍ

Nepovoluje se provádět jakoukoliv rekompilaci, transformaci, zpětnou analýzu, či jiné operace reverzního inženýrství, s výjimkou rozsahu výslovně povoleného v § 66 autorského zákona.

5. OCHRANNÉ ZNÁMKY

Toto ujednání neuděluje žádná práva ve spojení s ochrannými známkami společnosti MONET+ nad rámec vyčerpání práv dle §11 zákona o ochranných známkách.

6. VÝVOZNÍ OMEZENÍ

Uživatel bere na vědomí, že produkt podléhá Nařízení ES o režimu Společenství pro kontrolu vývozu, přepravy, zprostředkování a tranzitu zboží dvojího užití. Software ani žádná jeho část jakož i dokumentace nebudou jakýmkoliv způsobem vyvezeny (ve smyslu čl. 2 zmiňovaného nařízení) do jiné země bez povolení Ministerstva průmyslu a obchodu ČR.

7. REKLAMACE A ODBORNÁ POMOC

S žádostmi o odbornou pomoc k software a s reklamacemi se obracejte výlučně na dodavatele (poskytovatele) produktu.

8. DOKLAD KONCOVÉHO UŽIVATELE O LICENCI

Dokladem o legálním nabytí software je vždy a zásadně doklad o zaplacení licenčního poplatku (faktura) či jiné písemné ujednání o nabytí.

9. UKONČENÍ SMLOUVY

Porušení podmínek tohoto licenčního ujednání může mít za následek okamžité ukončení platnosti licence. V takovém případě musíte odinstalovat a zničit všechny kopie software a všechny jeho součásti.

10. VŠEOBECNÁ BEZPEČNOST

Za účelem efektivní ochrany systému před porušením bezpečnosti zabezpečení a před mallware, společnost MONET+ doporučuje pravidelné provádění záloh dat a systémových informací.

Doporučuje se použití všech dostupných funkcí zabezpečení, včetně, ale nikoliv pouze, antivirových programů, brány firewall, a instalace a používání dostupných aktualizací zabezpečení.

11. VYLOUČENÍ ODPOVĚDNOSTI

Omezená záruka: Společnost MONET+ ani jeho poskytovatelé tohoto software neodpovídají v žádném případě za škody ať už jakékoliv a to bez omezení, které by vznikly na základě nesprávného použití software.

V případě, že software nesplní podmínky omezené záruky (viz výše), máte právo na odstoupení od smlouvy a vrácení finanční náhrady ve výši zaplaceného licenčního poplatku, žádné další nároky se nepřiznávají.

12. ZŘEKNUTÍ SE ZÁRUK

Výše uvedená omezená záruka (v čl.11 tohoto ujednání), je jedinou výslovně poskytnutou zárukou a poskytuje se namísto veškerých dalších výslovných záruk či podobných závazků (pokud existují) vyplývajících z reklamních sdělení, dokumentace, sdělení na obalu a dalších sdělení.

13. ROZHODNÉ PRÁVO

Veškerá práva a povinnosti vyplývající ze vztahu mezi společností MONET+ a jakýmikoliv třetími osobami ve vztahu k software se řídí zákony České republiky a případné jeho vymáhání je možné pouze u Krajského soudu se sídlem ve Zlíně.

V případě, že bude jakékoli ustanovení těchto podmínek shledáno neúčinným, neplatným, nevymahatelným nebo nezákonným, zůstanou ostatní ustanovení nadále plně v platnosti a účinnosti.

Příloha č. 4 Smlouvy: Akceptační protokol

Akceptační protokol

Plnění / výstup: plnění nebo vystup, který je akceptován

Předáno dne: datum předání plnění

Předal / převzal	Role na projektu (koncepci), funkce	Podpis

Splnění akceptačních kritérií

Kritérium	Splnění kritéria

Akceptováno dne: datum akceptace

Výsledek akceptace: AKCEPTOVÁNO BEZ VÝHRAD / AKCEPTOVANO S VYHRADAMI / NEAKCEPTOVÁNO

Akceptoval	Role na projektu (koncepci), funkce	Podpis

Připomínky, výhrady: připomínky a výhrady k případnému plnění

Příloha č. 5 Smlouvy: Všeobecné obchodní podmínky pro poskytování služeb a Všeobecné obchodní podmínky pro dodávky zboží Objednatele

(Tato strana je úmyslně ponechána prázdná. VOP následují na další straně.)

Příloha č. 6 Smlouvy: Požadované technické parametry

Kategorie	Požadavek	Splněno	Komentáře, popis
	Popis hierarchie CA		
Architektura	Finální architektura se bude skládat z několika 2-úrovňových hierarchií CA. Počáteční hierarchie vypadá takto: 1.**Root RSA 1** a.***SubCA RSA QCA*** – kvalifikované certifikáty pro podpis a pečeť b.***SubCA RSA VCA*** – komerční osobní a serverové certifikáty 2.**Root ECC 11** a.***SubCA ECC QCA*** – kvalifikované certifikáty pro podpis a pečeť b.***SubCA ECC VCA*** – komerční osobní a serverové certifikáty 3.**Root ECC 21** a.***SubCA ECC TSA*** – kvalifikované certifikáty pro TSA 4.**Root ECC 31** a.***SubCA ECC QWAC*** – kvalifikované certifikáty QWAC 5.**Root ECC 41** a.***SubCA ECC TLS*** – komerční TLS certifikáty	ANO	V rámci dodávky lze vybudovat několik kořenových a vydávajících CA, vč. CA specializovaných na: - kvalifikované certifikáty pro podpis a pečeť - komerční osobní a serverové certifikáty - kvalifikované certifikáty pro TSA - kvalifikované certifikáty QWAC - komerční TLS certifikáty Komerční a kvalifikované CA budou odděleny. U každé CA bude možno (před instalací) rozhodnout, zda bude používat klíče RSA nebo ECC
	Technické požadavky		
Architektura	Root CA jsou fyzicky odděleny od vydávajících podřízených CA	ANO	Předpokládá se provoz root CA v offline režimu, zatímco podřízené online (=připojené k systémům PostSigunm).
Architektura	Podpora pro různé CA s RSA i ECC na jednom serveru	ANO	Na jednom virtualizačním serveru lze hostovat několik operačních systémů. V hostovaných operačních systémech mohou být provozovány různé CA s RSA nebo ECC.
Architektura	Řešení musí podporovat moduly Entrust nShield HSM ve variantách Solo a Connect až po novou generaci nShield 5.	ANO	Podpora přes ovladače k HSM. CA, popř. OCSP servery budou hostovat své klíče v nShield HSM. Operace se soukromými klíči budou probíhat v HSM. Pro vydávající CA doporučujeme použít síťové nShield Connect (nebo novější). Předpokládá se, že pro kvalifikované CA bude použito HSM a

			firmware s platnou certifikací Common Criteria EAL4 nebo vyšší.
Architektura	Řešení CA musí být provozuschopné na platformě MS Windows Server nebo Linux	ANO	Nabízené moduly (vč. CA) jsou určeny pro provoz na MS Windows Server 2016 nebo novějších.
Architektura	Podpora provozu DB přes 2 nezávislé lokality pro potřeby Disaster Recovery pracoviště, zejména pro službu OCSP	ANO	Databáze je provozována na platformě MS SQL Server. Lze ji provozovat v několika režimech vysoké dostupnosti, vč. např. replikace.
CRL/OCSP	Řešení musí podporovat RFC6960 a RFC5019	ANO	OCSP server funguje v souladu s uvedenými standardy.
CRL/OCSP	Řešení musí podporovat vytvoření samostatného respondéru OCSP pro všechny provozované certifikační autority v režimu vysoké dostupnosti nezávislého na službě CA. Služba OCSP bude k podepisování odpovědí používat vlastní certifikát.	ANO	OCSP server funguje jako samostatná služba, nezávislá např. na certifikační službě. Jedna instance může poskytovat informace o certifikátech z jedné nebo více CA. K jedné CA lze provozovat více instancí OCSP. OCSP získávají informace o stavu certifikátů z MSSQL DB (buď primární nebo repliky). OCSP podporují provoz v režimu Authorized responder, s vlastním certifikátem.
CRL/OCSP	Je požadováno zajištění dostatečného výkonu služby OCSP - je požadován min. výkon 100 odpovědí za 1 sekundu (v souhrnu za více instancí služby)	ANO	Požadovaný výkon byl experimentálně ověřen (vyžaduje dostatečný výkon DB, z níž se čerpají informace o certifikátech, a také odpovídají výkon HSM, které hostuje klíč OCSP).
CRL/OCSP	Řešení musí podporovat distribuci CRL na více CDP adres (min. 3) a jejich vydávání v předem nastaveném časovém harmonogramu i bezprostředně po zneplatnění certifikátu	ANO	Služba pro generování CRL umí zapisovat vydané CRL do více úložišť, protokolem SSH. Do vydávaných certifikátů lze uvádět více URL CDP/AIA (fixní seznam pro danou CA). Služba pro generování

			CRL vydává CRL pravidelně anebo jako reakci na revokaci (definovaný interval po revokaci).
CRL/OCSP	Podpora CRL v režimu, kdy odvolané certifikáty budou uvedeny v CRL i po vypršení platnosti samotného certifikátu	ANO	Konfiguračně lze ovlivnit, zda má služba pro generování CRL uvádět i expirované certifikáty, popř. jak daleko do minulosti.
Integrace	Dostupné a zdokumentované API pro vydávání certifikátů, kde bude možné předat všechny požadavky na daný certifikát kromě veřejného klíče, který bude součástí podepsané žádosti PKCS#10.	ANO	REST API nad protokolem HTTPS (vzájemná autentizace). Pro vydání certifikátu bude třeba dodat: žádost PKCS#10 a autorizovaná data, která se mají zapsat do certifikátu jako identifikační údaje držitele. Nabízené řešení dokáže z žádosti extrahovat veřejný klíč a doplnit do certifikátu identifikační údaje (subject, SAN), externsions, apod.. Přes stejné API lze zasílat také autorizované požadavky na revokaci certifikátů.
Integrace	rozhraní SOAP nebo REST API	ANO	REST API
Zabezpečení	Správa klíčových funkcí CA musí podporovat vícefaktorovou autentizaci pomocí certifikátů a fyzických kryptografických prostředků Klient aktuálně používá následující kryptografické prostředky a alespoň 2 z nich by měly být podporovány nativně nebo prostřednictvím knihoven PKCS#11 - eToken 5110 940 - TokenME - ProID+Q	ANO	Vícefaktová autentizace je podporována, s využitím nativních ovladačů pro CryptoAPI.
Zabezpečení	Řešení musí umožnit kontrolu duplicit veřejných klíčů při vydávání certifikátů a v případě duplicity veřejného klíče odmítnout vydání certifikátu.	ANO	Duplicita se kontroluje na úrovni MS SQL DB - unikátní index. Pokud by různé CA využívaly různé MS SQL DB (nepreferováno), pak se duplicita kontroluje jen v rámci podmnožiny, která sdílí stejnou DB.

Kryptografie	Software musí splňovat následující požadavky na podporu kryptografických algoritmů: Podpora asymetrických kryptografických algoritmů: RSA (PKCS#1 v1.5) RSA-PSS (Probabilistic Signature Scheme podle PKCS#1 v2.1) ECDSA (Elliptic Curve Digital Signature Algorithm) Podporované velikosti klíčů: RSA: 2048, 3072, 4096 bitů Eliptické křivky: P-256, P-384, P-521 (odpovídající standardům NIST FIPS 186-4) Podpora hashovacích funkcí: SHA-256 SHA-384 SHA-512 Software musí umožnit použití uvedených algoritmů a velikostí klíčů pro generování a ověřování digitálních podpisů, v souladu s aktuálními standardy a doporučeními pro bezpečnost kryptografických systémů.	ANO	Uvedené algoritmy a podpisová schémata jsou podporovány na úrovni CA, generování CRL i OCSP. Předpokládá se, že ovladače HSM adekvátně podporují dané algoritmy, a že HSM má zakoupeny licence pro podporu ECC.
Normy	Podpora min. RFC 5280, RFC 3647, RFC 3161, RFC 6960 a RFC 5019	ANO	Nabízené řešení funguje v souladu se standardy RFC 5280, RFC 6960 a RFC 5019. K nabízenému řešení lze zpracovat dokumentaci v souladu s RFC 3647, řešení bude fungovat s popsanými politikami a CPS. Z nabízené CA bude možno vydávat certifikáty pro TSA, v souladu RFC 3161. Certifikáty budou obsahovat položku Timestamp Authority.
Normy	Podpora evropské legislativy nařízení eIDAS a technických norem ETSI	ANO	Nabízené řešení bude implementováno v souladu s eIDAS a souvisejícími normami, zejména ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2.
Normy	Podpora standardů TLS a S/MIME dle CAB Forum	ANO	Nabízené řešení bude schopno do vydávaných certifikátů přidávat atributy a extesions podle potřeby (pro jednotlivé typy certifikátů). Včetně atributů a extensions vyžadovaných dle CAB Forum.

Normy	Řešení musí být certifikováno podle Common Criteria	ANO	Požadavek na Common Criteria certifikaci bude v nabízeném řešení splněno v souladu s klauzulemi OVR-6.5.2-01 a OVR-6.5.2-03 standardu ETSI EN 319 411-1.
Normy	Řešení musí podporovat rozšíření certifikátu včetně QC Statement	ANO	Nabízené řešení bude schopno do vydávaných certifikátů přidávat atributy a extesions podle potřeby (pro jednotlivé typy certifikátů). Včetně extensions QC Statement.
Normy	Řešení musí podporovat Certificate Transparency (CT)	ANO	Nabízené řešení podporuje zápis precertifikátů a certifikátů do CT Logů, v souladu se standardem RFC 6962. (Zápis do CT Logů lze aktivovat / deaktivovat pro jednotlivé typy certifikátů.)
TLS	Řešení musí podporovat rozdělené skupiny pro CT logy (google/nongoogle) a musí umožňovat nastavení min. počet odpovědí.	ANO	V konfiguraci CA bude možno definovat URL CTL Logů, do kterých mají být (pre-)certifikáty zapisovány. Lze definovat více URL a rozdělit je do skupin (google/nongoogle). Pro každou skupinu bude možno definovat min.počet odpovědí po kterých bude zápis do CT Logů považován za splněný. Získané struktury SCT se následně zapíší do finálních certifikátů.
	Licenční požadavky		
Jádro	Podpora více root certifikačních autorit na 1 fyzickém serveru – primární lokalita	ANO	Na jednom fyzickém serveru lze provozovat několik virtualizovaných OS, v každém jednu root CA. V případě nutnosti lze více root CA provozovat v jednom OS MS Windows Server, za podmínek: - V jednom okamžiku může být funkční jen jedna root CA - "Přepínání" mezi instancemi root CA

			vyžaduje servisní ukon (spuštění skriptu).
Jádro	Podpora více root certifikačních autorit na 1 fyzickém serveru – záložní lokalita	ANO	Technicky lze požadavek splnit - viz předchozí odpověď. Prakticky se nedoporučuje mít více instancí root CA na různých serverech, hrozí desynchronizace dat. V rámci havarijních plánů lze root CA zprovoznit v záložní lokalitě.
Jádro	Podpora na min. 7 vydávajících certifikačních autorit na alespoň 2 fyzických nebo virtuálních serverech – primární lokalita	ANO	Na jednom fyzickém serveru lze provozovat několik virtualizovaných OS, v každém jednu vydávající CA. Celkový počet podporovaných CA není (technicky) omezen. Počet hostovaných CA na jednom serveru je omezeno kapacitou fyzického hostitele. Při nedostatku kapacity bude nutno některé virtualizované OS přenést na jiné hostitele. V rámci projektu Dodavatel vyvine úsilí, aby bylo možno více CA provozovat v jednom OS MS Windows Server.
Jádro	Podpora na min. 7 vydávajícíní certifikačních autorit na alespoň 1 fyzickém nebo virtuálním serveru – záložní lokalita	ANO	Platí informace z předchozí odpovědi a navíc: Každá vydávající CA může běžet v několika instancích. Některé instance mohou běžet v primární a jiné v záložní lokalitě. Instance stejné CA musí sdílet jednu MS SQL databázi.
Jádro	Licence CA musí pokrývat i situace, kdy původní a nově vydávající CA fungují paralelně na stejném HW – délka takové koexistence může být až 3 roky v závislosti na platnosti vydaných certifikátů	ANO	Licence CA nejsou závislé na počtu souběžně platných certifikátů CA.
Jádro	Speciální licence pro 1 fyzický nebo virtuální neprodukční server pro provozování neprodukčních testovacích root CA (více na jednom serveru)	ANO	Součástí dodávky bude i licence pro provoz testovacích root CA (stejný počet jako produkčních root CA).
Jádro	Speciální licence pro 1 fyzický nebo virtuální server pro provozování neprodukčního testu vydávajících CA (více na jednom serveru)	ANO	Součástí dodávky bude i licence pro provoz testovacích CA (stejný

			počet jako produkčních CA).
Certifikáty	Řešení musí poskytovat licenci na uvedený počet certifikátů pro jednotlivé CA	ANO	Licence dodávaného řešení zahrnuje požadovaný počet pro jednotlivé CA.
Certifikáty	Licenční model musí odrážet situaci, kdy lze použít kombinace jednorázových a dlouhodobých certifikátů	ANO	Licenční model umožňuje vydávat jednorázové i dlouhodobé certifikáty.
Validace	Licence pro alespoň 3 produkční fyzické nebo virtuální servery pro provozování OCSP respondérů v režimu vysoké dostupnosti poskytující služby pro všechny provozované CA	ANO	Součástí dodávky bude i licence pro provoz produkčních OCSP pro všechny provozované CA. Licence umožní OCSP servery duplikovat (=provozovat v režimu vysoké dostupnosti).
Validace	Licence pro alespoň 1 neprodukční fyzický nebo virtuální server pro provozování testovacího OCSP respondéru	ANO	Součástí dodávky bude i licence pro provoz testovacích OCSP na alespoň jednom virtuálním OS.
	Požadavky na implementaci		
Implementace	Řešení musí být implementováno a dodáno v České republice	ANO	Česká republika je domovským státem dodavatele. Dodavatel předpokládá implementaci v ČR.
Implementace	Veškerá předložená projektová dokumentace musí být v českém nebo anglickém jazyce	ANO	Projektová dokumentace bude dodána v češtině.
Implementace	Technická dokumentace výrobku musí být k dispozici v českém nebo anglickém jazyce	ANO	Technická dokumentace bude dodána v češtině. Ve výjimečných případech může být část produktové dokumentace třetích stran (např. Microsoft) v angličtině.
	Požadavky na podporu		
Podpora	Řešení musí garantovat podporu a rozvoj řešení minimálně na dalších 5 let v souladu s evropskou legislativou (eIDAS) a jejími standardy	ANO	Dodavatel garantuje podporu a rozvoj řešení minimálně na dalších 5 let v souladu s evropskou legislativou (eIDAS) a jejími standardy.
Podpora	Dodavatel musí mít implementačního nebo servisního partnera v České republice	ANO	Česká republika je domovským státem dodavatele. Dodavatel bude zakázku i podporu realizovat vlastními pracovníky.
Podpora	Dodavatel musí být schopen nabídnout podporu SLA pro dodávané řešení minimálně v režimu 8x5	ANO	Dodavatel provozuje vlastní pracoviště servisní podpory. Je schopen zajistit podporu

			v režimu 8x5 nebo vyšším (po dohodě).

Příloha č. 7 – Požadavky na bezpečnost ICT – Pravidla pro dodavatele

1 Úvodní ustanovení

Česká pošta (dále jen ČP) zastává pozici odpovědné osoby ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**ZKB**“) a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**VKB**“), konkrétně je správcem kritické informační infrastruktury (dále jen „**KII**“). Dále pak je správcem či zpracovatelem osobních údajů dle Obecného nařízení o ochraně osobních údajů (dále jen „**GDPR**“) a zároveň je dle PCI DSS **"merchant"** (obchodník). ČP také provozuje systémy certifikovaní dle ISO 27001:2022.

Z důvodu udržení jednotnosti kybernetické bezpečnosti jsou požadavky definované ve výše uvedených legislativách a normách přenášeny a v relevantní míře aplikovány na všechny systémy provozované v rámci ICT ČP. V rámci ČP je nutné zajistit celistvost bezpečnostního standardu ICT infrastruktury a zabezpečit ji před potenciálními hrozbami a riziky v rámci řízení kybernetické bezpečnosti.

Kybernetická bezpečnost představuje inherentní a neoddělitelnou součást činností ČP. V souladu s platnými právními předpisy, normami a osvědčenými postupy pak ČP klade důraz na efektivní implementaci opatření týkajících se kybernetické bezpečnosti a tato opatření jsou vyžadována také v rámci činnosti dodavatelů. Tímto ČP zajišťuje dodržování nejnovějších standardů a osvědčených postupů v rámci celého dodavatelského řetězce, s cílem zajistit optimální ochranu informačních aktiv a udržení kybernetické odolnosti v digitálním prostředí.

1.1. Účel

Následující dokument stanovuje pravidla pro dodavatele ČP v souladu s ustanoveními ZKB, VKB a dalších příslušných vyhlášek, opatření a metodických pokynů za účelem zachování požadované úrovně kybernetické a informační bezpečnosti ČP a snížení bezpečnostních rizik spojených s přístupem dodavatelů k informačním aktivům ČP v rámci životního cyklu dodávky.

1.2. Přehled změn proti předchozí verzi

Jedná se o prvotní verzi dokumentu.

1.3. Zkratky a pojmy

POJMY	
Bezpečnost informací	Zachování důvěrnosti, integrity a dostupnosti informací.
Bezpečnostní událost	událost, která může způsobit nebo způsobila narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací
Bezpečnostní incident	narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku Bezpečnostní události
Dostupnost	Dostupnost informace v okamžiku její potřeby.
Důvěrnost	Dostupnost informace pouze oprávněným osobám.
Informační a komunikační technologie (ICT)	Veškerá technika, která se zabývá zpracováním a přenosem informací, a to je zejména výpočetní a komunikační technika (hardware i firmware) a programové vybavení (např. firemní aplikace, e-mail, cloudová a interní úložiště, Skype pro firmy, atd.)

Integrita	Zajištění správnosti a úplnosti informací.
Mobilní zařízení	Přenosný elektronický přístroj s různým programovým vybavením jako např. mobilní telefon, notebook, notebook, smartbook, PDA, tablet, USB zařízení apod.
pracovník	Zaměstnanci dodavatele a fyzické osoby v obdobném postavení (například DPP, DPČ, fyzická osoba na IČO apod.), kteří se podílí a/nebo mají podílet na plnění předmětu Smlouvy. Stanoví-li Pravidla povinnost pracovníkům dodavatele, dodavatel odpovídá za její s/plnění pracovníkem, průběžnou kontrolu a audit takového plnění a odpovídá za veškerou újmu způsobenou porušením takové povinnosti.
Uživatel	Každá fyzická osoba (včetně Pracovníků, zaměstnanců ČP nebo smluvně pověřených zaměstnanců externí fyzické nebo právnické osoby), které byl přidělen přístup k ICT ČP a příslušná přístupová oprávnění. Pro účely tohoto dokumentu se jedná o uživatele ICT ČP.
ZKRATKY	
ČP	Státní podnik Česká pošta (Česká pošta, s.p.).
GDPR	General Data Protection Regulation je nařízení Evropské unie.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
Politika ČP	Bezpečnostní politika ČP, jednotlivé dokumenty, které ji tvoří a část bezpečností dokumentace ČP, se kterými byl Dodavatel seznámen ze strany ČP pro účely plnění Smlouvy.
PCI DSS	Payment Card Industry Data Security Standard je soubor bezpečnostních standardů určených k ochraně údajů držitelů platebních karet.
Pravidla	Tato Pravidla pro dodavatele.
Smlouva	Hlavní smlouva uzavřená mezi ČP a dodavatelem. Součástí Smlouvy může být také dohoda o bezpečnostních aspektech při poskytování plnění uzavřená mezi ČP a Dodavatelem a/nebo vypracování dokumentů relevantních pro bezpečnost informací (bezpečnostní projekt, analýza rizik, softwarová analýza apod).
VKB	Vyhláška 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.
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

2. Organizace bezpečnosti informací

- Dodavatel je povinen užívat data, ke kterým získá přístup při plnění Smlouvy, jen k účelu, pro který byla poskytnuta a jen za podmínek, které byly pro jejich využití stanoveny Smlouvou, rovněž tak povinnost zachovávat důvěrnost dat, a to i po ukončení Smlouvy za podmínek dle Smlouvy.
- Dodavatel je povinen seznámit všechny své zaměstnance podílející se na plnění dle Smlouvy, bez ohledu na úroveň oprávnění, s požadavky dle těchto Pravidel pro dodavatele.
- Dodavatel je povinen poskytnout ČP veškerou součinnost nezbytnou k tomu, aby ČP řádně naplňovala právní povinnosti stanovené ZKB a VKB, opatřeními a metodikami NÚKIB (v rozsahu, v jakém jsou součástí Politiky ČP), a GDPR. Zejména se Dodavatel zavazuje poskytnout ČP součinnost směřující k zavedení a provádění bezpečnostních opatření podle ZKB, VKB a Politiky ČP.

- Dodavatel se zavazuje přijmout, udržovat a dokumentovat systém řízení bezpečnosti informací spočívající v přijetí dostatečných organizačních a technických opatření pro zajištění kybernetické a informační bezpečnosti, mít jej připravený na audit a kdykoliv jej na žádost ČP bezodkladně (nejdéle do 5 pracovních dnů) předložit. Taková žádost nebude zasílána dříve jak 30 dnů po uzavření Smlouvy.

3. Personální bezpečnost

- Dodavatel se zavazuje poskytnout ČP úplný jmenný seznam pracovníků Dodavatele, kteří se podílejí na předmětu plnění Smlouvy. V případě, že pracovníci Dodavatele mají přístup do perimetru Objednatele, a to ať už fyzický přístup či vzdálený přístup, tak se Dodavatel zavazuje informovat ČP o změnách v pracovnících a personálním zabezpečení Smlouvy v předstihu minimálně 5 pracovních dní.
- Dodavatel se zavazuje informovat ČP o ukončení pracovního nebo obdobného poměru pracovníků dodavatele, pro které byly u ČP vytvořeny přístupové účty, minimálně v předstihu 5 pracovních dní před ukončením takového poměru. Dodavatel je také povinen zvážit, zdali takový pracovník Dodavatele nepředstavuje po dobu výpovědní doby nebo obdobné doby bezpečnostní riziko (zejména s ohledem na důvod ukončení pracovního poměru či jiného druhu spolupráce) a případně přijmout opatření k zabránění zneužití přístupového účtu takovým pracovníkem Dodavatele (pokud je nutné zamezit přístup pracovníkovi ihned, oznámí to ČP).
- Dodavatel se zavazuje zavést systém prověřování uchazečů o zaměstnání a pracovníků, kteří se budou podílet na plnění pro ČP, aby zamezil vzniku potenciálního rizika v rámci přístupu k informačním a komunikačním systémům ČP.
- Dodavatel se zavazuje přijmout ve smlouvách se svými pracovníky odpovídající pravidla pro nakládání s informacemi, zachovávání kybernetické a informační bezpečnosti, zachování mlčenlivosti a zpracování osobních údajů v souladu s účinnými právními předpisy a poskytnout pracovníkům tato Pravidla pro dodavatele a smluvně či jiným podobným závazným způsobem (např. vnitřním předpisem) je zavázat k jejich dodržování.
- Pracovníci Dodavatele:
    - musí být seznámeni s těmito Pravidly s bezpečnostními požadavky Smlouvy;
    - mají dostatečné znalosti a praktické zkušenosti pro plnění přidělených úkolů;
    - mají veškeré potřebné zkoušky a atestace, které vyplývají ze zákona nebo požadavků regulátora a/nebo Smlouvy na druh práce, kterou mají v prostředí ČP vykonávat;
    - jsou Dodavatelem pravidelně školeni v oblastech bezpečnosti informací, kybernetické a informační bezpečnosti a právních a regulatorních požadavků relevantních pro naplnění předmětu Smlouvy;
    - kteří budou vstupovat nebo vjíždět do prostor ČP, musí být před započetím výkonu práce podrobeni ve smyslu právních předpisů školení o požární ochraně a bezpečnosti práce a současně musí být seznámeni s povinnostmi Dodavatele při pohybu v prostorách ČP.
- Dodavatel se zavazuje k vytvoření odpovídajícího disciplinárního procesu k přijetí opatření proti pracovníkům, kteří se dopustí porušení pravidel kybernetické a informační bezpečnosti v rámci nastaveného systému řízení kybernetické a informační bezpečnosti u Dodavatele a komunikovaných pravidel pro zajištění kybernetické a informační bezpečnosti ČP.

4. Fyzická bezpečnost

- Přístup pracovníků Dodavatele do prostor ČP je povolen, pouze pokud je jejich přítomnost nezbytná pro plnění pracovních povinností a na dobu nezbytně nutnou pro plnění pracovních povinností ze Smlouvy.
- Pracovníci Dodavatele jsou povinni se v prostorách ČP pohybovat pouze v doprovodu odpovědného zaměstnance ČP.
- Volný pohyb pracovníků Dodavatele v prostorách ČP je povolen pouze v případě, že dané osobě byla vystavena osobní přístupová karta. Pracovník Dodavatele je povinen přístupovou kartu chránit, mít ji

vždy při sobě na bezpečném místě, udržovat ji v místě odstíněném od potenciálního neoprávněného čtení (RFID ochrana) a není oprávněn přístupovou kartu dále zapůjčit jiným pracovníkům a/nebo třetím osobám a/nebo umožnit přístup jiných pracovníků a/nebo třetích osob do prostor ČP.

- Pracovníci Dodavatele nejsou oprávněni do prostředí ČP přinést zbraně, výbušniny, hořlaviny, bojové prostředky, jedy, radioaktivní a toxické látky, popř. jakékoli jiné látky ohrožující lidský život a/nebo zdraví.
- Bez písemného povolení ČP je zakázáno vynášení jakýchkoliv předmětů nepatřících pracovníkům Dodavatele a/nebo nesloužících k plnění Smlouvy, zejména jakékoliv dokumentace a/nebo paměťové médium (CD/DVD/Blu-ray disk, flash disk / paměťové karty, hard disk, zálohovací pásky apod.) z prostor ČP, popř. jiného místa plnění příslušné Smlouvy určeného Smlouvou, a jejich kopírování, fotografování, pořizování videozáznamů, připojování k jiným zařízením (než zařízení ČP) apod., pokud není ve Smlouvě anebo jinde písemně dohodnuto jinak.
- Přístup pracovníků Dodavatele do prostor ČP se zvýšeným stupněm bezpečnosti – chráněných zón (jako jsou serverové místnosti, datové místnosti, technické místnosti, trezor, pokladna apod.) je povolen pouze v doprovodu oprávněného zaměstnance ČP. Doprovod je nezbytný po celou dobu fyzické přítomnosti pracovníků Dodavatele v těchto prostorách a nepostačuje přístupová karta.
- V případě ztráty přístupové karty nebo v případě podezření ze ztráty přístupové karty je pracovník a/nebo Dodavatel povinen bezodkladně zajistit blokaci přístupové karty.
- Před vrácením zapůjčených paměťových médií Dodavateli musí být veškerá data ČP vymazána způsobem, který znemožňuje jejich opětovné obnovení; pokud toto nebylo provedeno ze strany ČP, je dodavatel povinen dané provést. O tomto je Dodavatel povinen sepsat protokol a na výzvu ČP jej bezodkladně (nejdéle do 5 pracovních dnů) předložit.
- Za prostory ČP se považují také prostory využívané ČP na základě smluvního vztahu s jejich vlastníkem a/nebo oprávněným uživatelem.

5. Řízení aktiv

- Dodavatel je povinen zpracovávat a uchovávat důvěrná data a informace související s předmětem plnění Smlouvy pouze na IT prostředcích, které jsou umístěny na území Evropské unie nebo Evropského hospodářského prostoru či USA, pokud tomu nebrání jiná legislativa.
- Dodavatel je povinen přistupovat k aktivům ČP pouze z prostředí a za použití prostředků dohodnutých ve Smlouvě; pokud nebyly dohodnuty ve Smlouvě, pak ze zabezpečeného prostředí a za použití důvěryhodných prostředků zabezpečených v souladu s CIS Benchmark z 50% a nejméně zabezpečených v souladu s minimálním bezpečnostním standardem vydaným NÚKIB a NAKIT. Za důvěryhodné se považují prostředí a prostředky, které jsou určené pro použití v podnikovém prostředí a jsou odpovídající pro plnění dle Smlouvy.
- Dodavatel bere na vědomí, že ČP má vlastní infrastrukturu IT s licenčním portfoliem, které podléhá nebo může podléhat smluvním závazkům se třetí stranou k celopodnikovému pokrytí. Dodavatel v rámci řešení bude, v případě dodávky sw licencí třetí strany, respektovat platné celopodnikové smluvní závazky ČP s dodavateli licenčních produktů a podpory.

6. Řízení přístupových oprávnění

- Dodavatel se zavazuje řídit všechna přístupová oprávnění v souladu s principem minimálního oprávnění („need to know“).
- Dodavatel se zavazuje zajistit jedinečnou identifikaci osob, popřípadě i aplikací s právem přístupu. Jedinečná identifikace osob musí být spravována v rámci centrálního IDM v souladu s požadavky Smlouvy a nejsou-li takové, pak s požadavky §19 VKB.
- Dodavatel se zavazuje na své straně evidovat přístup svých pracovníků k rozhraním, službám a prostředkům ČP, pokud jim byly pro plnění Smlouvy poskytnuty.

- Dodavatel se zavazuje neprodleně oznamovat veškeré personální a jiné změny u svých pracovníků podílejících se na plnění pro ČP, které jsou relevantní pro přidělování, změnu nebo odejmutí přístupového oprávnění přístupu do prostředí Objednatele.
- Dodavatel se zavazuje monitorovat a dokumentovat činnost svých pracovníků při užívání vlastních rozhraní, služeb a prostředků, pokud jsou tyto technické prostředky využívány k plnění Smlouvy.
- Dodavatel odpovídá v plném rozsahu za neoprávněné využití, resp. zneužití, přístupového oprávnění (včetně loginu, hesla, popř. i dalších přidělených přihlašovacích údajů, jako je PIN, certifikát, token).
- Dodavatel není oprávněn po ukončení příslušné Smlouvy, při jejímž plnění měl zřízeno a užíval přístupové oprávnění, nadále takové přístupové oprávnění užívat, a to bez ohledu na skutečnost, že takové přístupové oprávnění nebylo při ukončení příslušné Smlouvy ze strany ČP zrušeno. Pokud existuje mezi ČP a Dodavatelem více Smluv na různá nebo stejná plnění, a nedohodnou-li se ČP s Dodavatelem ve Smlouvě jinak, musí Dodavatel řídit oprávnění podle každé Smlouvy zvlášť a pracovníci musí mít individuální účty pro plněné každé Smlouvy zvlášť.
- Dodavatel si je vědom toho, že ČP může jednostranně odebrat přístup do prostředí ČP v případě porušení Politiky ČP, Smlouvy a/nebo Pravidel, v případě bezpečnostního incidentu nebo jiného chování ohrožujícího (včetně navýšení rizika) bezpečnost informací a/nebo aktiv ČP.
- Individuální účty musí být Dodavatelem vždy chráněny PIN nebo heslem (pokud jsou vydávány ze strany ČP, zajišťuje dané ČP). Heslo musí odpovídat minimálním požadavkům na hesla ČP a nejsou-li takové, pak minimálním požadavkům ZKB, VKB a metodických pokynů NÚKIB.

7. Bezpečnost provozu

- Dodavatel je povinen provádět pravidelný bezpečnostní monitoring IT svého prostředí, logovat události na svém prostředí a na rozhraní komunikace směrem k systémům ČP, pokud taková existují. Dále je povinen realizovat periodické ověřování zranitelností u aplikací a nástrojů komunikujících se systémy ČP a u souvisejících podpůrných aktiv.
- Dodavatel je povinen na svém prostředí implementovat tzv. bezpečnostní záplaty do aplikací, operačních systému, nástrojů pro ošetření zranitelností, a to bez zbytečného prodlení v případě zjištění jakékoliv zranitelnosti.
- V případech, kdy to bude žádoucí a vhodné, je Dodavatel povinen provádět i penetrační testování vlastního prostředí.
- Logování událostí sleduje a loguje minimálně:
    - datum a čas včetně specifikace časového pásma,
    - typ prováděné činnosti,
    - identifikaci technického aktiva, které činnost zaznamenalo,
    - jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
    - jednoznačnou síťovou identifikaci zařízení původce,
    - úspěšnost nebo neúspěšnost činnosti,
    - přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů (nebudou-li autentizovány pomocí AM - jako např. servisní účty aplikace, správcovské účty aj.),
    - úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
    - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
    - události vzešlé z činnosti uživatelů, které mohou mít vliv na bezpečnost digitalizace nebo vytěžování a manipulace s daty,
    - zahájení a ukončení činností technických aktiv,
    - kritická i chybová hlášení technických aktiv,
    - pokusy o přístup k záznamům monitorovacího SW o událostech a také pokusy o manipulaci se záznamy o událostech v něm a změny nastavení monitorovacích nástrojů pro zaznamenávání událostí,
    - synchronizaci jednotného času (pokud ji bude provádět sám a nespoléhat přitom na OS či časový server ČP).
- Dodavatel nesmí využívat přístup k systémům ČP, pokud takový existuje k jakýmkoli jiným aktivitám než k činnostem, které výslovně stanoví Smlouva.

8. Bezpečnost komunikací

- Dodavatel se zavazuje k zavedení bezpečnostních mechanismů k zajištění bezpečnosti sítě ve svém prostředí.
- V případě, že je Smlouvou a/nebo v rámci opatření pro snížení rizik navrženo zavedení šifrování, musí parametry kryptografických prostředků a povolené algoritmy naplňovat požadavky na šifrování dle Politiky ČP a nejsou-li takové, pak požadavky dle § 26 VKB Kryptografické prostředky a aktuální doporučení NÚKIB v oblasti kryptografických prostředků.
- Komunikace mezi prostředím Dodavatele a prostředím ČP musí probíhat pouze na zabezpečeném rozraní, které je monitorováno, není-li ve Smlouvě uvedeno jinak.

9. Bezpečnost vývoje

- Dodavatel je povinen se před započetím vývojových prací seznámit se softwarovými a hardwarovými technologiemi, které jsou v prostředí ČP podporované a používané. Dále je Dodavatel povinen si nechat odsouhlasit uvažované zdroje (hardware, software atd.), design/architekturu navrhovaného řešení a z toho vyplívající případné další požadavky, to vše za podmínek dle Smlouvy.
- Před započetím vývojových prací je Dodavatel povinen seznámit se s bezpečnostními a auditními požadavky ČP na vyvíjený software a odpovídající Politikou ČP.
- Dodavatel je povinen přistupovat k bezpečnosti informací jako k integrální součásti celého vývojového cyklu vývoje softwaru. Požadavky na informační bezpečnost musí být součástí analýzy požadavků na vyvíjený software, fáze plánování a návrhu vyvíjeného softwaru, a to ve vztahu k zamýšlenému nasazení a integraci do existujících procesů ČP.
- Dodavatel je povinen zajistit, aby veškerý vývoj byl v souladu s požadavky a pravidly bezpečného vývoje, přičemž je nutné uplatňovat osvědčené postupy (best practices) a mezinárodně uznávané standardy. Minimálním požadavkem je dodržování zásad definovaných v rámci normy ISO 27001, zaměřené na řízení bezpečnosti informací, a pravidel uvedených v OWASP (Open Web Application Security Project), které poskytují konkrétní doporučení pro prevenci zranitelnosti softwaru. Dodavatel je dále povinen pravidelně provádět bezpečnostní analýzy a testování vyvíjeného softwaru, například penetrační testy, a zajistit, že budou identifikované zranitelnosti bezodkladně odstraněny.
- Dodavatel se zavazuje v rámci vývoje a testování používat pouze testovací data vytvořená/dodaná v souladu se Smlouvou; testování na ostrých datech je vyloučeno. Testovací data zároveň musí být anonymizovaná, leda je nezbytné využít neanonymizovaných dat a takový postup je dopředu s ČP dohodnut.
- Pokud není ve Smlouvě uvedeno jinak, součástí vývojových prací je i dodání úplné dokumentace dodaného software, včetně:
    - dokumentace architektury/designu – zahrnuje vztahy k prostředí a stavebním základům, které budou použity v návrhu softwarových komponent (pokud je tvořena analýza, pak analýzu po aktualizaci dle skutečného provedení);
    - technická dokumentace – dokumentace kódu, soupis použitých open source zdrojů, popis rozhraní a API;
    - bezpečnostní dokumentace – dokumentace chyb a zranitelností dle metodiky OWASP, výsledky penetračního testování,
    - uživatelská dokumentace – manuály pro koncového uživatele, systémové administrátory a osazenstvo podpory;
    - příručka pro administraci, instalaci a údržbu;
    - programátorskou dokumentaci (vývojové postupy, diagramy apod.).
- Dodavatel musí ČP proaktivně upozornit na všechny jemu známé skutečnosti spojené s vývojem a chováním dodaného kódu, které by po nasazení mohly negativně ovlivnit běh v produkčním prostředí a/nebo návazné systémy.
- Dodavatel odpovídá za životní cyklus programového kódu a souvisejících aktiv v tom smyslu, že ČP bude včas podrobně informována o jejich stavu, využití, potřebnosti apod., vč. zranitelností a jakýchkoli bezpečnostních rizicích.

10. Řízení poddodavatelů

- Dodavatel se zavazuje zavést pravidla výběru a postupy pro řízení a evidenci svých poddodavatelů, podílejících se na plnění této zakázky v souladu s pravidly a postupy ČP.
- Dodavatel se zavazuje využít pro plnění zakázky pouze bezúhonné subjekty a osoby, na jejichž straně nestojí žádné bezpečnostní překážky (ve smyslu kybernetické bezpečnosti).
- Dodavatel se zavazuje přenést na tyto subjekty povinnost poskytnout veškerou potřebnou součinnost pro provedení hodnocení rizik.
- Dodavatel se zavazuje své poddodavatele smluvně či podobným způsobem zavázat k dodržování těchto Pravidel, Politiky ČP a dalších povinností v oblasti bezpečnosti informací vyplývajících ze Smlouvy v rozsahu, v jakém je k nim zavázán sám.

11. Řízení bezpečnostních incidentů

- Dodavatel je povinen vyhodnocovat bezpečnostní události svých aplikací a nástrojů a jeho souvisejících podpůrných aktiv, které se podílejí na této zakázce a mohou ovlivnit bezpečnost ČP.
- Dodavatel je povinen nahlásit ČP podezření na bezpečnostní zranitelnosti, bezpečnostní události nebo bezpečnostní incidenty vzniklé v jakékoliv souvislosti s plněním povinností Dodavatele, ať už by k tomu došlo při užívání rozhraní, služeb a prostředků ČP anebo na straně Dodavatele či jeho poddodavatele (či kterékoliv jiné osoby, např. pracovníků), které jsou relevantní pro zachování bezpečnosti informací aktiv ČP (včetně schopnosti způsobit změnu v hodnocení rizik) a/nebo by mohly mít negativní vliv na předmět plnění nebo ohrozit chod IS ČP. Pokud je v takovém případě možné přijmout opatření k zabránění vzniku bezpečnostního incidentu, je Dodavatel povinen je přijmout (na svém prostředí a/nebo plnění dle Smlouvy) a doporučit ČP kroky k přijetí takových opatření (na ostatním prostředí ČP).
- Dodavatel je povinen oznámit ČP a evidovat každý bezpečností incident vzniklý v jakékoliv souvislosti s plněním povinností Dodavatele, ať už by k tomu došlo při užívání rozhraní, služeb a prostředků ČP anebo na straně Dodavatele či jeho poddodavatele (či kterékoliv jiné osoby, např. pracovníků), které jsou relevantní pro zachování bezpečnosti informací aktiv ČP (včetně schopnosti způsobit změnu v hodnocení rizik) a/nebo by mohly mít negativní vliv na předmět plnění nebo ohrozit chod IS ČP. Dodavatel je povinen oznámit takový bezpečností incident nejpozději do čtyř (4) hodin po jeho zjištění. Dodavatel zároveň sdělí ČP opatření, která již provedl ve vztahu k tomuto bezpečnostnímu incidentu, aby ČP mohla případně splnit svou ohlašovací povinnost dle legislativy jako je zejména GDPR, ZKB, PCI DSS, ale i smluvních požadavků svých klientů.
- Dodavatel je povinen ohlásit jednotlivý bezpečnostní incident nebo událost současně všemi následujícími způsoby:
    - e-mailem na e-mailovou adresu uvedenou ve Smlouvě;
    - telefonicky na telefonní číslo uvedené ve Smlouvě; a
    - na Helpdesk ČP.

12. Kontinuita činností

- Dodavatel je povinen mít zaveden plán obnovy pro aplikace a systémy provozované Dodavatelem a přímo ovlivňující plnění Smlouvy.
- Pro relevantní ICT aktiva Dodavatele, která jsou používána pro anebo v souvislosti s plněním Smlouvy, je Dodavatel povinen zajistit vhodný cyklus zálohy dat, který splňuje smluvně ujednané požadavky dle Smlouvy. Přitom musí Dodavatel posoudit minimálně následující:
    - plán zálohy;
    - umístění záloh (zálohy musí být ukládány v jiné oblasti, než zálohována data);
    - metody zálohování, formáty dat a médií;
    - retenční období pro zálohování;
    - ověřování integrity záloh;

- postupy obnovení a testování, včetně harmonogramů obnovy v případě narušení;
- použití šifrování;
- oddělení záloh v cloudovém prostředí s více zákazníky;
- frekvence a metody revize procesů pro zálohování a obnovu;
- dokumentace záloh a jejich obsahu, včetně označování médií.

- Zálohovaná data musí být chráněna před neoprávněným přístupem. Tato data musí být chráněna dalšími bezpečnostními opatřeními, které vyžaduje jejich klasifikace (úroveň).

13. Zabezpečení mobilních zařízení

- Mobilní zařízení, skrz které mají pracovníci a/nebo Dodavatel přístup k aktivům ČP a/nebo na nich mají uložena aktiva ČP, musí nad rámec dalších požadavků uvedených v těchto Pravidlech, splňovat v tomto článku níže uvedené požadavky.
- Mobilní zařízení musí být vždy chráněno proti neautorizovanému použití vhodnými prostředky jako je PIN, heslo, biometrika.
- Mobilní zařízení musí být adekvátním způsobem chráněna proti:
  - narušení bezpečnosti dat a informací ČP.
  - zneužití třetími osobami (průnik do systému, aplikací atp.);
  - ztrátě nebo poškození (zničení, odcizení nebo poškození dat nebo výpočetní techniky atp.);
  - neoprávněnému použití (přístup k důvěrným informacím, službám, technických prostředků atp.);
  - použití, které není v souladu s účelem jejich pořízení a/nebo účelem, pro které jim byl umožněn přístup k aktivům ČP; a
  - útokům třetích stran (škodlivé programové vybavení, hackerské útoky, nezáplatované zranitelnosti atp.).
- Dodavatel je povinen vrátit užívané mobilní zařízení ČP (pokud mu bylo ze strany ČP předáno) ve stavu, ve kterém je převzal, s přihlédnutím k běžnému opotřebení, při ukončení Smlouvy, popř. dříve, byl-li o to ze strany ČP výslovně požádán, a to vždy bez prodlení.

14. Soulad s pravidly pro dodavatele

- Dodavatel se zavazuje k součinnosti v rámci pravidelných kontrol ze strany ČP, které mají za cíl ověřit soulad procesů a postupů s těmito Pravidly, a to za podmínek dle Smlouvy.

15. Požadavky na dodávku

- Dodávaný SW musí generovat bezpečnostní události v souladu minimálně s požadavky ZoKB a § 22 VoKB.
- Bezpečnostní události musí být zasílány do SIEM systému Objednatele, konkrétně za pomoci Syslog a ve formátu Common Event Format (CEF).
- Dodávaný SW musí splňovat požadavky na odolnost vůči útokům, a to implementací relevantních pravidel dle OWASP, pokud některé požadavky nemohou být naplněny, musí být o tomto záznam v rámci předávané dokumentace včetně relevantního odůvodnění a výslovně na toto musí být upozorněno.
- Dodavatel je povinen zajistit pravidelné zajišťování záplat/oprav dodaného SW:
  - Aplikace záplat pro kritické zranitelnosti musí být implementovány nejpozději do 30 kalendářních dnů od jejich zveřejnění.
- Předmět plnění bude podrobován pravidelnému testování skeneru zranitelnosti Tenable, a to minimálně čtyřikrát ročně. Povinností Dodavatele je:
  - Vyhodnocení výsledků těchto testů, včetně analýzy identifikovaných zranitelností.

  - Odstranění všech zjištěných problémů v souladu s jejich závažností, přičemž kritické a vysoké zranitelnosti musí být odstraněny bez zbytečného odkladu, nejpozději však do 90 kalendářních dnů od jejich identifikace.
- Systém jehož je dodávka součástí bude podroben pravidelnému ročnímu penetračnímu testování formou Gray boxu testu, přičemž:
  - Penetrační testování bude rovněž součástí akceptačního procesu OS.
  - Dodavatel je povinen odstranit veškeré zjištěné nedostatky, případně předložit odůvodnění nemožnosti jejich odstranění spolu s návrhem dodatečných opatření k odstranění zjištěné zranitelnosti a výsledného rizika.
  - Dodavatel je povinen spolupracovat v přípravě testování, jeho realizaci a následném odstraňování zjištěných nedostatků. Tato spolupráce zahrnuje zejména:
    - Poskytnutí potřebné dokumentace, přístupů a součinnosti pro provedení testů.
    - Podporu při interpretaci výsledků testů a návrzích opatření.
    - Aktivní účast při implementaci navržených opatření a přijetí kroků pro minimalizaci rizik.

16. Změnové řízení

- Dodavatel je povinen vést podrobnou dokumentaci všech konfiguračních změn v informačním systému, infrastruktuře nebo softwaru.
- Dokumentace musí obsahovat:
  - Popis změny.
  - Důvod změny.
  - Očekávaný dopad na systém.
  - Datum provedení změny.
  - Osobu odpovědnou za provedení změny
  - Popis postupu pro návrat do předchozího stavu.
- Všechny změny podléhají předchozímu schválení Objednatelem prostřednictvím definovaného procesu změnového řízení.
- Dodavatel je povinen poskytnout Objednateli veškeré relevantní informace nezbytné k rozhodnutí o schválení změny.
- Dodavatel je povinen spolupracovat s Objednatelem na změnové řízení při jakékoliv plánované změně.
- Proces změnového řízení bude zahrnovat:
  - Identifikaci změny.
  - Analýzu dopadů na systém a služby.
  - Návrh opatření pro minimalizaci rizik.
  - Vyhodnocení nákladů a přínosů.
- Dodavatel je povinen aktivně spolupracovat s Objednatelem při plánování, analýze a implementaci změn.
- Dodavatel nese odpovědnost za správné provedení změn dle schváleného plánu změnového řízení.
- Veškeré změny musí být prováděny způsobem, který minimalizuje přerušení provozu.
- Dodavatel je povinen pravidelně aktualizovat dokumentaci na základě provedených změn.
- Aktualizovaná dokumentace musí být předána Objednateli v předem dohodnutém formátu a termínu.
- Veškeré kroky související s prováděním změn musí být plně auditovatelné.
- Dodavatel je povinen uchovávat záznamy o změnách po dobu stanovenou Smlouvou.
- Dodavatel musí Objednatele včas informovat o všech plánovaných změnách, jejich průběhu a případných odchylkách od plánu.
- V případě mimořádných událostí (např. havárií) musí být Objednatel neprodleně informován.
- V případě neplánovaných změn (např. reakce na kritický incident) musí být změna zpětně zdokumentována a projednána s Objednatelem.
- Dodavatel musí prokázat, že změna byla nezbytná a provedena v souladu s procesy minimalizace rizik.

- Dodavatel je povinen informovat personál Objednatele o důsledcích změn, pokud tyto změny ovlivňují provozní činnosti nebo užívání systému.