

ZADÁVACÍ DOKUMENTACE

ve smyslu § 28 odst. 1 písm. b) zákona č. 134/2016 Sb., o zadávání veřejných zakázek,
ve znění pozdějších předpisů (dále jen „ZZVZ“)

pro nadlimitní veřejnou zakázku na dodávky a služby

„Dodávka loadbalanceru a aplikačního firewallu“

zadávanou v otevřeném řízení podle § 56 ZZVZ

(dále jen „veřejná zakázka“).

Identifikační údaje veřejné zakázky:

Název veřejné zakázky	Dodávka loadbalanceru a aplikačního firewallu
Druh veřejné zakázky	Dodávky a služby
Druh zadávacího řízení	Otevřené řízení
Režim veřejné zakázky	Nadlimitní
Lhůta pro podání nabídek	19. září 2024 do 10:00 hod.
Způsob podání nabídek	Elektronicky prostřednictvím Národního elektronického nástroje
Předpokládaná hodnota	7.256.000 Kč bez DPH

Identifikační údaje zadavatele:

Název	Česká republika – Český telekomunikační úřad
Sídlo	Sokolovská 58/219, Praha 9
IČO	701 06 975
Zastoupený/á	Ing. Marek Ebert, předseda Rady ČTÚ
Právní forma	Organizační složka státu
DPH – plátce / neplátce	Osoba identifikovaná k dani
Profil zadavatele	https://sluzby.e-zakazky.cz/Profil-Zadavatele/c6503add-b4cd-409d-87ce-7b7b867ccf65

Kontaktní osoba zadavatele:

Kontaktní osoba	Mgr. Jan Kroj
Telefonní kontakt	+420 224 004 711
E-mailová adresa	kroj@ctu.cz

PREAMBULE

Zadání této veřejné zakázky se řídí právními předpisy České republiky, zejména ZZVZ.

Podáním nabídky dodavatel zcela a bez výhrad akceptuje podmínky účasti v zadávacím řízení, podmínky průběhu zadávacího řízení, pravidla pro hodnocení nabídek, požadavky zadavatele na obsah, formu a způsob podání nabídky a případné další zadávací podmínky, které zadavatel stanovil v zadávací dokumentaci.

Od dodavatelů se očekává, že si pečlivě prostudují, splní a dodrží veškeré podmínky, pokyny a termíny vyplývající ze zadávací dokumentace. Práva a povinnosti neuvedené v této zadávací dokumentaci se řídí ZZVZ. Zadavatel nemůže vzít v úvahu žádnou výhradu účastníka zadávacího řízení k zadávacím podmínkám obsaženou v jeho nabídce.

1. PŘEDMĚT PLNĚNÍ VEŘEJNÉ ZAKÁZKY

1.1. Předmět plnění veřejné zakázky

Předmětem plnění veřejné zakázky je kompletní dodávka, instalace a konfigurace webového aplikačního firewallu (WAF) a loadbalanceru dle Technické specifikace, která je přílohou č. 1 Závazného vzoru smlouvy obsaženého v příloze č. 2 zadávací dokumentace.

Podrobná specifikace předmětu plnění veřejné zakázky je uvedena v příloze č. 2 zadávací dokumentace (Závazný vzor smlouvy) a v přílohách Závazného vzoru smlouvy.

1.2. Klasifikace předmětu veřejné zakázky (CPV kódy)

Předmět plnění	CPV kód
Servery	48820000-2
Implementace programového vybavení	72263000-6

2. PŘEDPOKLÁDANÁ HODNOTA VEŘEJNÉ ZAKÁZKY

Předpokládaná hodnota veřejné zakázky byla stanovena v souladu s § 16, 20 písm. a) a § 21 odst. 1 písm. b) ZZVZ a činí celkem 7.256.000 Kč bez daně z přidané hodnoty (DPH).

Předpokládaná hodnota zahrnuje veškeré náklady spojené s plněním předmětu veřejné zakázky.

3. DOBA A MÍSTO PLNĚNÍ

3.1. Místo plnění veřejné zakázky

Místem plnění veřejné zakázky je sídlo zadavatele.

3.2. Doba plnění veřejné zakázky

Začátek plnění: ode dne účinnosti smlouvy

Doba plnění: dodávka zařízení včetně instalace, konfigurace a školení nejpozději do 46 pracovních dní ode dne účinnosti smlouvy

podpora dodaného zařízení po dobu 60 měsíců ode dne akceptace.

4. POSKYTNUTÍ A VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE

4.1. Poskytnutí zadávací dokumentace

Textová část zadávací dokumentace v elektronické podobě je všem dodavatelům k dispozici bez omezení přístupu na profilu zadavatele (<https://sluzby.e-zakazky.cz/profil-zadavatele/c6503add-b4cd-409d-87ce-7b7b867ccf65/zakazka/P24V00000017>). Zadavatel dodavatele upozorňuje na skutečnost, že zadávací dokumentace je souhrnem požadavků zadavatele, a nikoliv konečným souhrnem veškerých požadavků vyplývajících z obecně známých platných právních předpisů a odborných norem. Dodavatel se tak musí při zpracování své nabídky vždy řídit nejen požadavky obsaženými v zadávací dokumentaci, ale též ustanoveními příslušných obecně závazných norem.

4.2. Změna nebo doplnění zadávací dokumentace

Zadávací podmínky obsažené v zadávací dokumentaci může zadavatel změnit nebo doplnit před uplynutím lhůty pro podání nabídek. Změna nebo doplnění zadávacích podmínek musí být uveřejněna nebo oznámena dodavatelům stejným způsobem jako zadávací podmínka, která byla změněna nebo doplněna.

Pokud to povaha doplnění nebo změny zadávacích podmínek vyžaduje, zadavatel současně přiměřeně prodlouží lhůtu pro podání nabídek. V případě takové změny nebo doplnění zadávacích podmínek, která může rozšířit okruh možných dodavatelů, prodlouží zadavatel lhůtu tak, aby od odeslání změny nebo doplnění zadávací dokumentace činila nejméně celou svou původní délku.

4.3. Vysvětlení zadávací dokumentace

Dodavatelé jsou oprávněni po zadavateli písemně požadovat vysvětlení zadávací dokumentace, a to v souladu s § 98 ZZVZ. Zadavatel vysvětlení uveřejní na svém profilu, odešle nebo předá včetně přesného znění žádosti bez identifikace tohoto dodavatele, a to za podmínek uvedených v § 98 ZZVZ.

5. OBCHODNÍ A PLATEBNÍ PODMÍNKY

Obchodní podmínky zadavatele včetně platebních jsou obsaženy v příloze č. 2 zadávací dokumentace ve formě Závazného vzoru smlouvy (dále také jen „smlouva“).

Veškeré obchodní a platební podmínky určené zadavatelem v této zadávací dokumentaci jsou zadavatelem stanoveny jako závazné. Dodavatelé jsou povinni respektovat a ve svých nabídkách splnit veškeré podmínky a požadavky zadavatele vymezené zadávacími podmínkami a plně respektovat podmínky uvedené v Závazném vzoru smlouvy.

Závazný vzor smlouvy obsahuje „žlutě podbarvená“ místa, která budou dodavatelem v návrhu smlouvy obsaženém v nabídce doplněna v souladu s obsahem podané nabídky. Dodavatel není oprávněn v návrhu smlouvy měnit či doplňovat jakékoliv údaje s výjimkou údajů doplňovaných do těchto žlutě podbarvených míst.

6. DALŠÍ PODMÍNKY PRO UZAVŘENÍ SMLOUVY

Vybraný dodavatel (účastník zadávacího řízení, který bude vybrán k uzavření smlouvy) bude vyzván zadavatelem postupem podle § 122 odst. 4 písm. a) ZZVZ k předložení originálů nebo úředně ověřených kopií dokladů o jeho kvalifikaci, pokud je nepředložil již v rámci nabídky.

7. VYUŽITÍ PODDODAVATELE

Zadavatel neomezuje rozsah případných poddodávek během plnění této veřejné zakázky.

Zadavatel v souladu s § 105 odst. 1 písm. b) ZZVZ požaduje, aby dodavatel ve své nabídce předložil seznam poddodavatelů, pokud jsou dodavateli známi a uvedl, kterou část a v jakém finančním rozsahu veřejné zakázky bude každý z poddodavatelů plnit. Tím není dotčena výlučná odpovědnost dodavatele za poskytování řádného plnění.

8. KVALIFIKACE DODAVATELŮ

8.1. Požadavky zadavatele na kvalifikaci dodavatele

Kvalifikovaným pro plnění veřejné zakázky je dodavatel, který prokáže splnění:

- a) základní způsobilosti podle § 74 ZZVZ,
- b) profesní způsobilosti podle § 77 ZZVZ a
- c) technické kvalifikace podle § 79 ZZVZ.

8.2. Kvalifikace v případě společné účasti dodavatelů

V případě společné účasti dodavatelů prokazuje základní způsobilost a profesní způsobilost podle § 77 odst. 1 ZZVZ každý dodavatel samostatně.

8.3. Prokázání kvalifikace prostřednictvím jiných osob

Dodavatel může ve smyslu § 83 ZZVZ prokázat určitou část technické kvalifikace nebo profesní způsobilosti s výjimkou kritéria podle § 77 odst. 1 ZZVZ prostřednictvím jiných osob. Dodavatel je v takovém případě povinen zadavateli předložit:

- a) doklady prokazující splnění profesní způsobilosti podle § 77 odst. 1 ZZVZ jinou osobou,
- b) doklady prokazující splnění chybějící části kvalifikace prostřednictvím jiné osoby,
- c) doklady o splnění základní způsobilosti podle § 74 ZZVZ jinou osobou a
- d) smlouvu nebo jinou osobou podepsané potvrzení o její existenci, jejímž obsahem je písemný závazek jiné osoby k poskytnutí plnění určeného k plnění veřejné zakázky nebo k poskytnutí věcí nebo práv, s nimiž bude dodavatel oprávněn disponovat při plnění veřejné zakázky, a to alespoň v rozsahu, v jakém jiná osoba prokázala kvalifikaci za dodavatele.

Způsob prokázání se řídí požadavky § 83 odst. 2 až 5 ZZVZ.

8.4. Doba prokazování splnění kvalifikace / pravost a stáří dokladů

Doklady prokazující základní způsobilost podle § 74 a profesní způsobilost podle § 77 odst. 1 ZZVZ musí prokazovat splnění požadovaného kritéria způsobilosti nejpozději v době 3 měsíců přede dnem zahájení zadávacího řízení.

Doklady prokazující splnění kvalifikace je dodavatel oprávněn předložit v kopii, nikoliv však ve formě čestného prohlášení, pokud tak výslovně nepřipouští ZZVZ nebo tato zadávací dokumentace.

Před uzavřením smlouvy je vybraný dodavatel povinen předložit originál nebo ověřené kopie dokladů o kvalifikaci, pokud již nebyly předloženy v zadávacím řízení, a to v souladu s § 45 odst. 1 a § 46 odst. 1 ZZVZ.

8.5. Základní způsobilost

Způsobilým není dodavatel, který:

- a) byl v zemi svého sídla v posledních 5 letech před zahájením zadávacího řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 ZZVZ nebo obdobný

trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží,

- b) má v České republice nebo v zemi svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
- c) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
- d) má v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti,
- e) je v likvidaci, proti němuž bylo vydáno rozhodnutí o úpadku, vůči němuž byla nařízena nucená správa podle jiného právního předpisu nebo v obdobné situaci podle právního řádu země sídla dodavatele.

Je-li dodavatelem právnická osoba, musí podmínku podle písm. a) splňovat tato právnická osoba a zároveň každý člen statutárního orgánu. Je-li členem statutárního orgánu dodavatele právnická osoba, musí podmínku podle písm. a) splňovat tato právnická osoba, každý člen statutárního orgánu této právnické osoby a osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

Je-li dodavatelem pobočka závodu zahraniční právnické osoby, musí podmínku podle písm. a) splňovat tato právnická osoba a vedoucí pobočky závodu. Je-li dodavatelem pobočka závodu české právnické osoby, musí podmínku podle písm. a) splňovat osoby uvedené v předchozím odstavci a vedoucí pobočky závodu.

Dodavatel prokazuje splnění podmínek základní způsobilosti ve vztahu k České republice předložením:

- a) výpisu z evidence Rejstříku trestů ve vztahu k § 74 odst. 1 písm. a) ZZVZ,
- b) potvrzení příslušného finančního úřadu ve vztahu k § 74 odst. 1 písm. b) ZZVZ,
- c) písemného čestného prohlášení ve vztahu ke spotřební dani ve vztahu k § 74 odst. 1 písm. b) ZZVZ,
- d) písemného čestného prohlášení ve vztahu k § 74 odst. 1 písm. c) ZZVZ,
- e) potvrzení příslušné okresní správy sociálního zabezpečení ve vztahu k § 74 odst. 1 písm. d) ZZVZ,
- f) výpisu z obchodního rejstříku, nebo předložením písemného čestného prohlášení v případě, že není v obchodním rejstříku zapsán, ve vztahu k § 74 odst. 1 písm. e) ZZVZ.

Zadavatel doporučuje použít k prokázání části základní způsobilosti (§ 74 odst. 1 písm. b), c) a e) ZZVZ), kterou lze podle § 75 odst. 1 písm. c), d) a f) ZZVZ prokázat čestným prohlášením, vzorový formulář, který je uvedený v příloze č. 3 zadávací dokumentace.

8.6. Profesní způsobilost

Dodavatel prokazuje splnění profesní způsobilosti ve vztahu k České republice předložením výpisu z obchodního rejstříku nebo jiné obdobné evidence, pokud jiný právní předpis zápis do takové evidence vyžaduje.

Doklady prokazující splnění profesní způsobilosti nemusí dodavatel předložit, pokud právní předpisy v zemi jeho sídla obdobnou profesní způsobilost nevyžadují.

8.7. Technická kvalifikace

Dodavatel prokáže splnění technické kvalifikace předložením:

- 1) **seznamu významných dodávek/služeb podle § 79 odst. 2 písm. b) ZZVZ**, poskytnutých dodavatelem za poslední 3 roky před zahájením zadávacího řízení.

Zadavatel vymezuje minimální úroveň pro doložení čestného prohlášení o řádném poskytnutí a dokončení (tj. dodávka/služba, jejíž poskytování bylo řádně dokončeno, nebo služba trvajících, poskytovaná nepřetržitě po dobu nejméně 1 roku) významných dodávek/služeb obdobného charakteru (dodání a podpora HW a SW), jako je předmět této veřejné zakázky tak, že dodavatel splní tuto technickou kvalifikaci, pokud uvede alespoň dvě významné dodávky/služby, přičemž každá z uvedených významných dodávek/služeb musí být o minimálním finančním objemu 5.000.000 Kč bez DPH. Doba trvání podpory HW a SW alespoň u jedné uvedené významné dodávky/služby musí být soustavně trvajících minimálně 12 měsíců.

Za významnou dodávku/službu lze pro účely prokázání kritérií technické kvalifikace dle § 79 odst. 2 písm. b) ZZVZ považovat výhradně takovou zakázku, jejíž realizace nebyla objednatelem předčasně ukončena (zejména odstoupením od smlouvy) z důvodu porušení smluvních či zákonných povinností na straně dodavatele.

Pro splnění požadavku předloží dodavatel čestné prohlášení – Seznam významných dodávek/služeb. Z předloženého Seznamu významných dodávek/služeb bude zřejmé splnění požadavků zadavatele, tedy:

- a) název dodávky/služby,
- b) identifikace objednatele,
- c) popis/předmět dodávky/služby,
- d) cena v Kč bez DPH,
- e) měsíc a rok zahájení a ukončení dodávky/služby,
- f) telefonický a e-mailový kontakt na objednatele dodávky/služby.

Seznam musí být podepsán osobou oprávněnou zastupovat dodavatele.

K prokázání splnění této části technické kvalifikace je možno využít formulář, který je přílohou č. 4 (Seznam významných dodávek/služeb) této zadávací dokumentace.

Pozn. zadavatele: V souladu s § 39 odst. 5 ZZVZ je zadavatel oprávněn ověřovat věrohodnost poskytnutých údajů a dokladů a může si je také opatřovat sám. Zadavatel si vyhrazuje právo kontroly a posouzení toho, zda je seznam významných dodávek/služeb předložený dodavatelem pravdivý a zda jsou splněny všechny podmínky týkající se významných dodávek/služeb. V případě, že údaje uvedené dodavatelem budou v rozporu s výsledky kontroly zadavatele, vyhrazuje si zadavatel právo dodavatele ze zadávacího řízení vyloučit.

- 2) **jmenného seznamu osob (členů realizačního týmu) podle § 79 odst. 2 písm. c) a d) ZZVZ**, které se budou podílet na plnění veřejné zakázky (bez ohledu na to, zda jde o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli), a to včetně osvědčení o jejich vzdělání a odborné kvalifikaci.

Dodavatel prokáže splnění tohoto kritéria kvalifikace předložením seznamu členů realizačního týmu (včetně uvedení informace, zda se jedná o zaměstnance dodavatele nebo osobu působící jako poddodavatel / zaměstnanec poddodavatele).

Zadavatel požaduje prokázat splnění této části technické kvalifikace v následující minimální úrovni:

Dodavatel musí mít pro plnění veřejné zakázky k dispozici realizační tým složený z certifikovaných odborníků pro tyto oblasti podpory:

- WAF,
- Loadbalanceru.

Dodavatel prokáže splnění tohoto kvalifikačního předpokladu předložením seznamu osob a certifikátem vystaveným dodavatelem nebo výrobcem nabízeného zařízení. Jeden člen realizačního týmu může pokrýt více požadovaných znalostí.

8.8. Další podmínky prokazování kvalifikace

Změny v kvalifikaci dodavatele:

Pokud po předložení dokladů nebo prohlášení o kvalifikaci dojde v průběhu zadávacího řízení ke změně kvalifikace dodavatele, je dodavatel povinen tuto změnu zadavateli ve lhůtě do 5 pracovních dnů oznámit a do 10 pracovních dnů od oznámení této změny předložit nové doklady nebo prohlášení ke kvalifikaci; zadavatel může tyto lhůty prodloužit nebo prominout jejich zmeškání. Povinnost podle věty první dodavateli nevzniká, pokud je kvalifikace změněna takovým způsobem, že:

- a) podmínky kvalifikace jsou nadále splněny a
- b) nedošlo k ovlivnění kritérií hodnocení nabídek.

Dozví-li se zadavatel, že dodavatel nesplnil povinnost uvedenou v odstavci 1 tohoto článku, zadavatel jej bezodkladně vyloučí ze zadávacího řízení.

Seznam kvalifikovaných dodavatelů:

Dodavatelé zapsaní v seznamu kvalifikovaných dodavatelů jsou oprávněni v souladu s § 228 ZZVZ prokázat splnění základní způsobilosti a profesní způsobilosti předložením výpisu ze seznamu kvalifikovaných dodavatelů. V případě profesní způsobilosti tento výpis nahrazuje doklad prokazující splnění profesní způsobilosti v tom rozsahu, v jakém údaje ve výpisu ze seznamu kvalifikovaných dodavatelů prokazují splnění kritéria profesní způsobilosti. Výpis ze seznamu kvalifikovaných dodavatelů nesmí být starší než 3 měsíce od posledního dne, ke kterému má být základní a profesní způsobilost prokázána.

Zadavatel nemusí přijmout výpis ze seznamu kvalifikovaných dodavatelů, na kterém je vyznačeno zahájení řízení podle § 231 odst. 3 ZZVZ. V takovém případě zadavatel vyzve dodavatele k objasnění dokladů podle § 46 odst. 1 ZZVZ.

Stejně jako výpisem ze seznamu kvalifikovaných dodavatelů může dodavatel prokázat kvalifikaci osvědčením, které pochází z jiného členského státu, v němž má dodavatel sídlo, a které je obdobou výpisu ze seznamu kvalifikovaných dodavatelů.

Systém certifikovaných dodavatelů:

Dodavatelé mohou rovněž v souladu s § 234 ZZVZ prokázat splnění kvalifikace nebo její části platným certifikátem vydaným v rámci schváleného systému certifikovaných dodavatelů, a to v rozsahu uvedeném na certifikátu.

Stejně jako certifikátem může dodavatel prokázat kvalifikaci osvědčením, které pochází z jiného členského státu, v němž má dodavatel sídlo, a které je obdobou certifikátu vydaného v rámci systému certifikovaných dodavatelů.

9. PODMÍNKY SESTAVENÍ A PODÁNÍ NABÍDEK

9.1. Požadavky na formu a obsah zpracování nabídek

Nabídka musí být podána výhradně elektronicky způsobem, který je uveden v bodu 10 zadávací dokumentace.

Dodavatel může podat pouze jednu nabídku. Dodavatel, který podal nabídku v zadávacím řízení, nesmí být současně poddodavatelem, jehož prostřednictvím jiný dodavatel v tomtéž zadávacím řízení prokazuje kvalifikaci. Pokud dodavatel podá více nabídek samostatně nebo společně s dalšími dodavateli, nebo je poddodavatelem, jehož prostřednictvím jiný dodavatel

v tomtéž zadávacím řízení prokazuje kvalifikaci, zadavatel všechny nabídky podané takovým dodavatelem vyřadí. Dodavatele, jehož nabídka byla vyřazena, zadavatel bezodkladně vyloučí z účasti v zadávacím řízení a neprodleně o vyloučení, včetně uvedení důvodu, dodavatele písemně informuje.

Nabídka bude zpracována tak, aby byla dobře čitelná, a nebude obsahovat opravy a přepisy, které by zadavatele mohly uvést v omyl.

9.2. Jazyk nabídky

Nabídka, všechny ostatní doklady a dokumenty s ní související a veškerá korespondence musí být v českém jazyce. Cizojazyčné listiny dokládající kvalifikační předpoklady (s výjimkou dokladů o vzdělání a případných certifikátů podle bodu 8.7 odst. 2 této zadávací dokumentace) musí být opatřeny překladem do českého jazyka. Doklady ve slovenském jazyce se předkládají bez překladu.

9.3. Požadavky na sestavení nabídky – členění a pořadí obsahu nabídek

Nabídka musí obsahovat veškeré dokumenty požadované ZZVZ a zadavatelem v zadávací dokumentaci.

Zadavatel doporučuje dodavatelům, aby zpracovali nabídku v následujícím členění:

- a) obsah nabídky,
- b) krycí list nabídky (identifikační údaje dodavatele, kontaktní osoba, nabídková cena; v podobě, jejíž vzor je uveden v příloze č. 1 této zadávací dokumentace),
- c) doklady k prokázání splnění základní způsobilosti (výpis ze seznamu kvalifikovaných dodavatelů, anebo doklady podle bodu 8.5 této zadávací dokumentace),
- d) doklady k prokázání splnění profesní způsobilosti (doklad podle bodu 8.6 této zadávací dokumentace),
- e) doklady prokazující splnění technické kvalifikace (podle bodu 8.7 této zadávací dokumentace),
- f) návrh smlouvy podepsaný osobou oprávněnou zastupovat dodavatele, který bude po obsahové stránce odpovídat Závaznému vzoru smlouvy, který je přílohou č. 2 této zadávací dokumentace, a ve kterém budou dodavatelem doplněny žlutě podbarvené části (včetně příslušných příloh),
- g) další dokumenty (např. plná moc pro oprávněnou osobu, smlouva s poddodavatelem, smlouva o společnosti) apod.,
- h) prohlášení o počtu stran s podpisem oprávněné osoby.

10. ZPŮSOB, LHŮTA A MÍSTO PRO PODÁNÍ NABÍDEK

Nabídka musí být podána výhradně elektronicky prostřednictvím zadavatelem určeného elektronického nástroje, kterým je Národní elektronický nástroj (NEN) - <https://nen.nipez.cz/>, a to nejpozději do 19. září 2024 do 10:00 hod. Jiné podání nabídky nebude považováno za řádné.

Pro elektronické podání nabídky je nutno být ze strany dodavatele registrován v elektronickém nástroji NEN. Podrobné instrukce na požadavky a podmínky pro podání nabídky prostřednictvím elektronického nástroje NEN jsou dostupné pod odkazem <https://nen.nipez.cz/> v sekci Uživatelské příručky.

K zašifrování nabídky musí být dodavatelem použit veřejný klíč s certifikátem, který je zadavatelem uveřejněn společně se zadávací dokumentací v rámci dokumentů příslušné veřejné zakázky v elektronickém nástroji NEN.

11. ZADÁVACÍ LHŮTA

V souladu s § 40 odst. 1 ZZVZ zadavatel stanovil zadávací lhůtu, po kterou dodavatelé zadávacího řízení nesmí ze zadávacího řízení odstoupit, v délce trvání 3 měsíců.

Počátkem běhu zadávací lhůty je konec lhůty pro podání nabídek. Zadávací lhůta neběží po dobu, ve které zadavatel nesmí uzavřít smlouvu s vybraným dodavatelem podle § 246 ZZVZ.

12. OTEVÍRÁNÍ NABÍDEK V ELEKTRONICKÉ PODOBĚ

Otevírání nabídek v elektronické podobě se řídí § 108 a § 109 ZZVZ a bude neveřejné.

13. HODNOTICÍ KRITÉRIA

Základním hodnoticím kritériem veřejné zakázky je ekonomická výhodnost nabídek podle § 114 ZZVZ.

Hodnocena bude celková cena v Kč bez DPH za celou dobu plnění uvedená dodavatelem v rámci tabulky v Krycím listu nabídky, resp. čl. III odst. 1 Závazného vzoru smlouvy, který je přílohou č. 2 této zadávací dokumentace.

V případě rovnosti nejvýhodnějších cen rozhodne o vítězi los.

14. POSOUZENÍ SPLNĚNÍ PODMÍNEK ÚČASTI

V rámci posouzení splnění podmínek účasti zadavatel posoudí, zda dodavatelé nebo pouze vybraný dodavatel splňují podmínky účasti v souladu s § 37 ZZVZ stanovené ZZVZ a v této zadávací dokumentaci, tj. zda splňují:

- a) základní způsobilost podle § 74 ZZVZ,
- b) profesní způsobilost podle § 77 odst. 1 ZZVZ,
- c) splnění technické kvalifikace podle § 79 odst. 2 písm. b) až d) ZZVZ,
- d) splnění smluvních podmínek podle § 37 odst. 1 písm. c) ZZVZ,
- e) splnění podmínek týkajících se nabídky podle § 37 odst. 2 ZZVZ.

Splnění podmínek účasti v zadávacím řízení prokáže dodavatel:

- podle písmene a) až c) způsobem uvedeným v bodu 8 této zadávací dokumentace,
- podle písmene d) předložením podepsaného návrhu smlouvy, který bude po obsahové stránce odpovídat Závaznému vzoru smlouvy, který je přílohou č. 2 této zadávací dokumentace, zadávacím podmínkám a obsahu nabídky dodavatele, a
- podle písmene e), pokud splní podmínky zadavatele pro zpracování a podání nabídky uvedené v bodech 9 a 10 této zadávací dokumentace.

U vybraného dodavatele musí zadavatel provést posouzení splnění podmínek účasti v zadávacím řízení a hodnocení jeho nabídky vždy.

V souladu s § 46 odst. 1 ZZVZ může zadavatel po dodavateli požadovat, aby v přiměřené lhůtě objasnil předložené údaje nebo doklady, nebo doplnil další či chybějící údaje anebo doklady.

15. OCHRANA PROTI NESPRÁVNÉMU POSTUPU ZADAVATELE

15.1. Námitky

Námitky může podat dodavatel, kterému postupem zadavatele souvisejícím se zadáváním veřejné zakázky hrozí nebo vznikla újma. Přípustnost námitek, jejich podávání, lhůty, jakož i náležitosti a přezkum jsou upraveny v § 241 a násl. ZZVZ.

Námítky se podávají písemně a musí splňovat obsahové náležitosti podle § 244 ZZVZ.

Námítky proti zadávacím podmínkám lze v souladu s § 242 odst. 5 zákona podat nejpozději 72 hodin před skončením lhůty pro podání nabídek (pozn.: tato lhůta byla „připočtena“ k původně zadavatelem stanovené přiměřené lhůtě pro podání nabídek).

Zadavatel přezkoumá podané námítky v plném rozsahu a ve lhůtě do 15 dnů od obdržení námitek odešle stěžovateli písemné rozhodnutí o tom, zda námítkám vyhovuje nebo je odmítá, s uvedením důvodu.

15.2. Přezkoumání úkonů zadavatele

Přezkoumávání úkonů zadavatele Úřadem pro ochranu hospodářské soutěže je upraveno v § 248 a násl. ZZVZ.

16. VYHRAZENÁ PRÁVA ZADAVATELE

Zadavatel nepřipouští varianty nabídky.

Zadavatel nepožaduje poskytnutí jistoty.

Zadavatel si vyhrazuje právo si v rámci součinnosti vybraného dodavatele před podpisem smlouvy tohoto vyzvat, aby předložil informace o úrovni kybernetické bezpečnosti na straně dodavatele, resp. jeho případných poddodavatelů při realizaci veřejné zakázky. Poskytnutí informací požaduje zadavatel za účelem maximálního přijatelného zajištění dat a informací zadavatele, které mohou být v rámci plnění veřejné zakázky uloženy a zpracovávány v ICT prostředí dodavatele, neboť narušení bezpečnosti těchto dat a informací by mohlo mít potenciální dopad na provoz kritické infrastruktury a kritických či významných informačních systémů zadavatele, a v důsledku způsobit nedodržení požadavků stanovených zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, ze strany zadavatele.

Vybraný dodavatel před podpisem smlouvy předloží jím vyplněnou tabulku uvedenou v příloze č. 5 (Informace o zajištění KB dodavatele a poddodavatelů) zadávací dokumentace. Tabulku v tomto rozsahu vyplní rovněž každý poddodavatel, tzn. dodavatel a jeho případný poddodavatel vyplní každý vlastní tabulku podle stavu bezpečnosti jejich ICT prostředí.

Zadavatel upozorňuje, že je v postavení ústředního správního úřadu pro výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací, poštovních služeb a služeb dodávání balíků.

Vzhledem k tomu, že součástí poskytovaných služeb bude jak konfigurace prvků za ochrannými prostředky proti úniku informací, přes které mohou být v nešifrované podobě přenášeny informace, tak zpracovávání informací a dat, jejichž znalost by mohla zvýhodnit některý ze subjektů podnikajících v elektronických komunikacích, v oblasti poštovních služeb, v oblasti služeb dodávání balíků nebo v rozhlasovém či televizním vysílání, bude zadavatel při posouzení nabídek dodavatelů, kteří podnikají v elektronických komunikacích ve smyslu § 8 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, v poštovních službách ve smyslu § 17 zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů, v oblasti služeb dodávání balíků ve smyslu čl. 2 bodu 3) nařízení Evropského parlamentu a Rady (EU) 2018/644 o službách přeshraničního dodávání balíků, či jsou provozovateli rozhlasového a/nebo televizního vysílání podle § 3 odst. 1 a § 2 odst. 1 písm. c), e) a f) zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, ve znění pozdějších předpisů, posuzovat ve smyslu § 79 odst. 1 ZZVZ, zda takový dodavatel (či jeho případný poddodavatel/poddodavatelé, kteří se budou podílet na konfiguraci dodávaných technologií, nebo během plnění veřejné zakázky budou mít prostřednictvím dodávaných

technologií přístup k síti zadavatele) nemá protichůdné zájmy, které by mohly negativně ovlivnit plnění veřejné zakázky.

Zadavatel v souladu s § 113 ZZVZ posoudí, zda nabídka neobsahuje mimořádně nízkou nabídkovou cenu. K tomu zadavatel uvádí, že za mimořádně nízkou nabídkovou cenu bude v případě ceny za 1 člověkodenní (MD) plnění na objednávku cena nižší než 9.000 Kč bez DPH.

Zadavatel je dále oprávněn:

- a) nevracet dodavateli podanou nabídku,
- b) neposkytovat dodavateli náhradu nákladů spojených s účastí v zadávacím řízení,
- c) zrušit výběrové řízení v souladu s § 127 ZZVZ.

17. PŘÍLOHY ZADÁVACÍ DOKUMENTACE

Přílohy zadávací dokumentace tvoří následující dokumenty:

Příloha č. 1 – Krycí list nabídky

Příloha č. 2 – Závazný vzor smlouvy

Příloha č. 3 – Vzorek čestného prohlášení (základní způsobilost)

Příloha č. 4 – Vzorek seznamu významných dodávek/služeb

Příloha č. 5 – Informace o zajištění KB dodavatele a poddodavatelů (tabulka)

V Praze dne 16. srpna 2024

Ing. Marek Ebert v. r.
předseda Rady
Českého telekomunikačního úřadu

Za správnost: Mgr. Jan Kroj, 19. 8. 2024

KRYCÍ LIST NABÍDKY

ZÁKLADNÍ ÚDAJE:

Název veřejné zakázky: Dodávka loadbalanceru a aplikačního firewallu
Zadavatel: Česká republika – Český telekomunikační úřad
Sídlo: Sokolovská 58/219, Praha 9 - Vysočany
IČO: 701 06 975
Jejímž jménem jedná: Ing. Marek Ebert, předseda Rady ČTÚ
Kontaktní osoba a email: Mgr. Jan Kroj, tel.: 224 004 711, e-mail: kroj@ctu.cz

Identifikační údaje o dodavateli				
Obchodní firma nebo název / jméno a příjmení	...			
Sídlo / místo podnikání	...			
Právní forma	...			
Zastoupena	...			
IČO	...			
DIČ	...			
Kontaktní osoba	...			
Telefon	...			
E-mail	...			
Malý nebo střední podnik	ano / ne			
Nabídková cena	Cena v Kč bez DPH	Sazba DPH	Částka DPH	Cena v Kč včetně DPH
Dodání 2 kusů appliance zapojených ve vysoké dostupnosti	...	...	...	...
SW moduly zajišťující požadované funkce, SW pro centrální management včetně příslušných licencí s platbou za 5 let	...	...	...	...
Instalace, konfigurace, zaškolení	...	...	...	...
Servisní podpora na 5 let, včetně práce na zaintegrování jednotlivých IS v objemu 150 MD (man-day)	...	...	...	...
5 let RMA podpory 10x5xNBD pro 2 kusy appliance zapojených ve vysoké dostupnosti	...	...	...	...
Celkem	...	...	...	...

V dne

.....
 Jméno a podpis osoby oprávněné zastupovat dodavatele

**Smlouva č. CTU/2024_0055
na dodávku loadbalanceru a aplikačního firewallu**

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku,
ve znění pozdějších předpisů (dále jen „smlouva“)

mezi těmito smluvními stranami:

1. Česká republika – Český telekomunikační úřad

se sídlem: Sokolovská 58/219, Praha 9
adresa pro doručování: pošt. přihrádka 02, 225 02 Praha 025
bankovní spojení: Česká národní banka, pobočka Praha
Číslo účtu: 725001/0710
IČO: 70106975
DIČ: CZ70106975 (osoba identifikovaná k dani)
jejímž jménem jedná: Ing. Marek Ebert,
předseda Rady Českého telekomunikačního úřadu

(dále jen „Objednatel“ nebo „ČTÚ“) na straně jedné

a

2.

se sídlem:
zastoupen:
IČO:
DIČ:
bankovní spojení:
číslo účtu:
zapsaná v obchodním rejstříku vedeným soudem v, oddíl ..., vložka ...

(dále jen „Dodavatel“) na straně druhé,

společně označované také jako „strany“ nebo jednotlivě též jako „strana“.

**Článek I.
Účel a předmět smlouvy**

1. Účelem této smlouvy je stanovení obsahových požadavků, postupů, obchodních podmínek a dalších smluvních ujednání, na jejichž základě proběhne dodávka a instalace loadbalanceru a aplikačního firewallu, to vše v návaznosti na výsledky zadávacího řízení na veřejnou zakázku s názvem „Dodávka loadbalanceru a aplikačního firewallu“.
2. Objednatel má v plánu rozšířit stávající infrastrukturu o zařízení typu ADC (Application delivery controller), který zajistí vysokou dostupnost aplikací prostřednictvím loadbalancingu a zároveň zvýší jejich úroveň ochrany pomocí aplikačního firewallu (WAF).
3. Předmětem smlouvy je na straně jedné závazek Dodavatele dodat Objednateli 2 kusy appliance (webový aplikační firewall [WAF] a loadbalancer) zapojených ve vysoké dostupnosti (tzv. HA), a to včetně dodávky veškerých potřebných provozních licencí, instalace, konfigurace, integrace a zajištění záručního servisu a podpory plnění po dobu 60 měsíců ode dne akceptace dodávky. Podrobná specifikace předmětu plnění je uvedena v příloze č. 1 této smlouvy. Na straně druhé je předmětem smlouvy závazek Objednatele za řádně a včas poskytnuté plnění zaplatit Dodavateli sjednanou cenu.

Článek II. Místo a čas plnění

1. Místem plnění je sídlo Objednatele.
2. Dodání zařízení včetně instalace, konfigurace a školení nejpozději do 46 pracovních dnů ode dne účinnosti smlouvy. Podpora dodaného zařízení po dobu 60 měsíců ode dne akceptace plnění podle první věty.

Článek III. Cena a platební podmínky

1. Celková cena za plnění dle čl. I odst. 3 této smlouvy a dle cenové kalkulace uvedené v příloze č. 2 této smlouvy, činí Kč bez DPH. Celková cena bude hrazena postupně takto:
 - a) cena za plnění dle bodu 1 a 3 přílohy č. 2 této smlouvy (Cenová kalkulace) za dodávku, implementaci a zaškolení činí ... Kč bez DPH,
 - b) cena za servisní podporu po dobu 5 let, včetně práce na zaintegrování jednotlivých IS v objemu 150 MD (man-day) dle bodu 4 přílohy č. 2 této smlouvy (Cenová kalkulace) činí ... Kč bez DPH, tj. ... Kč bez DPH/1 MD (man-day),
 - c) cena za SW moduly zajišťující všechny funkce, SW pro centrální management včetně příslušných licencí dle bodu 2 přílohy č. 2 této smlouvy (Cenová kalkulace) činí ... Kč bez DPH,
 - d) cena za 5 let RMA podpory 10x5xNBD pro 2 kusy appliance zapojených ve vysoké dostupnosti dle bodu 5 přílohy č. 2 této smlouvy (Cenová kalkulace) činí ... Kč bez DPH.
2. Ceny jsou stanoveny v měně CZK jako pevné a lze je měnit pouze při změně sazby DPH. K ceně bude při její fakturaci připočtena DPH v aktuální výši ke dni zdanitelného plnění. Ceny zahrnují veškeré náklady Dodavatele nezbytné pro plnění smlouvy.
3. Cena za plnění bude hrazena následujícím způsobem:
 - a) cena dle odstavce 1 písm. a), c) a d) tohoto článku bude uhrazena po převzetí řádného plnění Objednatelům na základě podepsání příslušného akceptačního protokolu, který bude přílohou příslušné faktury vystavené Dodavatelem,
 - b) cena dle odstavce 1 písm. b) tohoto článku bude hrazena jako součin skutečného rozsahu poskytnutých služeb (MD) a jednotkové ceny dle odstavce 1 písm. b) tohoto článku. Podkladem pro stanovení skutečné hodnoty poskytnuté služby je podepsaný výkaz práce (viz odstavec 5 tohoto článku), jehož kopie bude přílohou daňového dokladu – faktury (dále jen „faktura“).
4. Splatnost faktury je sjednána na 21 dnů ode dne doručení Objednateli. V případě faktury doručené Objednateli mezi 20. prosincem a 10. lednem je taková faktura splatná nejdříve následujícího 1. února. Platební povinnosti Objednatele plynoucí z této smlouvy jsou splněny dnem odepsání příslušné částky ve prospěch účtu Dodavatele. Úhrada bude provedena bezhotovostním převodem z účtu Objednatele ve prospěch účtu Dodavatele.
5. Všechny faktury musí mít náležitosti podle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a § 435 OZ, a musí obsahovat číslo této smlouvy. Přílohou faktury musí být příslušný akceptační protokol (pro plnění dle odstavce 1 písm. a), c) a/nebo d) tohoto článku smlouvy), potažmo podepsaného výkazu práce servisní podpory (pro plnění dle odstavce 1 písm. b) tohoto článku smlouvy) potvrzující poskytnutí služeb v daném období či rozsahu. Objednatel je oprávněn fakturu Dodavateli vrátit bez zbytečného odkladu po zjištění, že obsahuje údaje nesprávné nebo chybí-li některá ze zákonem či touto smlouvou požadovaných náležitostí, a to před uplynutím

doby splatnosti, aniž by došlo k prodloužení s jeho úhradou. Nová doba splatnosti počíná běžet ode dne vystavení bezvadné faktury.

Článek IV.

Ostatní podmínky plnění smlouvy, práva a povinnosti smluvních stran

1. Dodavatel zajistí provedení následujících činností v rozsahu minimálně:
 - a) zpracování projektové dokumentace, plány a harmonogram postupu projektu,
 - b) přípravné práce a příprava HW včetně validace umístění technologií do cílového místa – místo v racku, napájení, konektivita atd.,
 - c) fyzická instalace zařízení na dohodnuté místo za předem dohodnutých podmínek,
 - d) základní konfigurace interface, routingu a návazných síťových služeb,
 - e) instalace SW včetně potřebných licencí,
 - f) rozšířená konfigurace jednotlivých komponent a nasazení příslušných politik web aplikačního firewallu ve spolupráci se Objednatelem,
 - g) v případě potřeby implementace příslušných HW/SW update od výrobce,
 - h) dokumentace skutečného provedení,
 - i) provedení akceptačních testů,
 - j) plnění dle této smlouvy bude Dodavatel Objednateli poskytovat nejpozději v termínech uvedených v příloze č. 4 této smlouvy. Ve stanovených termínech musí být plnění Dodavatele poskytnuto řádně, tj. musí být poskytnuto v takové kvalitě, která již nebude vyžadovat jakékoliv následné odstraňování vad či nedostatků. Dodavatel se zavazuje nejméně 1 pracovní den předem písemně uvědomit kontaktní osobu objednatel uvedenou v čl. XI odst. 5 písm. a) této smlouvy o předpokládaném termínu předání, instalace či konfigurace plnění nebo jeho části. Objednatel do 3 pracovních dnů ode dne předání plnění Dodavatelem potvrdí převzetí řádného plnění podepsáním příslušného akceptačního protokolu nebo ve stejné lhůtě v rámci akceptačního protokolu vytkne Dodavateli zjištěné vady. Způsob a termín jejich odstranění bude navržen Dodavatelem s tím, že určení termínu pro odstranění vad a nedostatků nemá vliv na povinnost Dodavatele dodat řádné plnění nejpozději do termínu ve smyslu čl. II odst. 2 této smlouvy; odstranění zjištěných vad a nedostatků bude opětovně ověřeno a výsledek bude zaznamenán formou samostatného zápisu v akceptačním protokolu).
2. Další podmínky plnění smlouvy:
 - a) veškeré nabízené plnění musí být plně kompatibilní se současnou infrastrukturou Objednatel,
 - b) součástí veškerého nabízeného plnění musí být i všechny potřebné licence (HW/SW), jež budou zahrnuty ve sjednané ceně,
 - c) veškerý dodaný HW musí být nový, nepoužitý a určený výrobcem pro český trh,
 - d) SW licence musí být bez jakýchkoli právních vad, Objednatel nepřipouští produkty třetích stran (tzv. OEM kompatibilní),
 - e) Dodavatel musí být certifikovaný partner výrobce pro Českou republiku.
3. Dodavatel je dále po celou dobu trvání této smlouvy zajistit:
 - a) plnění veškerých povinností vyplývajících z právních předpisů České republiky, zejména pak předpisů pracovněprávních, předpisů v oblasti zaměstnanosti, a dále

oblasti bezpečnosti a ochrany zdraví při práci, a to vůči všem osobám, které se budou podílet na plnění této smlouvy,

b) dodržování zákona č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon), ve znění pozdějších předpisů,

c) řádné a včasné plnění finančních závazků vůči svým případným poddodavatelům.

Plnění uvedených povinností zajistí poskytovatel i u svých případných poddodavatelů.

4. Objednatel je povinen zajistit:

a) aby zařízení a software byly užívány v souladu se specifikacemi a návody výrobce,

b) poskytnou Dodavateli v přiměřené lhůtě nezbytně nutnou součinnost při provádění činností servisu a údržby.

5. V případě úmyslu Dodavatele či jeho poddodavatele zahájit podnikání ve smyslu § 8 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, v poštovních službách ve smyslu § 17 zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů, v oblasti služeb dodávání balíků ve smyslu čl. 2 bodu 3) nařízení Evropského parlamentu a Rady (EU) 2018/644 o službách přeshraničního dodávání balíků, ani nejsou provozovatelé rozhlasového a/nebo televizního vysílání podle § 3 odst. 1 a § 2 odst. 1 písm. c), e) a f) zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, ve znění pozdějších předpisů, je Dodavatel povinen předem písemně informovat Objednatele.

Článek V.

Vyšší moc a okolnosti vylučující odpovědnost

1. Smluvní strany nebudou odpovědné za částečné nebo úplné neplnění smluvních závazků následkem okolností vylučujících odpovědnost v případech tzv. vyšší moci.
2. Výraz vyšší moc znamená a zahrnuje zejména: přírodní katastrofu, požár, záplavy, zemětřesení a dále povstání, stávky, pracovní boje jakéhokoliv druhu nebo terorismus, které mají přímou souvislost a brání plnění povinností ze smlouvy a plnění povinností nelze zajistit jinak nebo je nahradit, nehody, pád letadla včetně nehod, kterým se nedalo vyhnout v souvislosti s plněním této smlouvy včetně přijetí zákona nebo mimořádného rozhodnutí přísl. úřadu v souvislosti se zásahem vyšší moci, pokud příčiny a události mají vliv na plnění povinností stran ze smlouvy a plnění povinností vyplývajících ze smlouvy nelze zajistit jinak.
3. Vyskytne-li se působení překážky, s níž jsou spojeny účinky vylučující odpovědnost, lhůty ke splnění smluvních závazků se prodlouží o dobu trvání takové překážky. Smluvní strana, která je postižena takovou překážkou, je však povinna okamžitě, písemně, uvědomit druhou smluvní stranu o této skutečnosti, o začátku trvání této překážky a předpokládané době jejího trvání.

Článek VI.

Ochrana informací

1. Objednatel a Dodavatel se zavazují, že obchodní, technické, jakož i netechnické informace, které mají nebo by mohly mít potenciální hodnotu, a které jim byly svěřeny smluvním partnerem, nezpřístupní třetím osobám bez předchozího písemného souhlasu druhé smluvní strany a nepoužijí tyto informace ani pro jiné účely než pro plnění svých závazků podle podmínek této smlouvy. Za důvěrnou informaci se pokládá vždy taková informace, která je takto kteroukoliv smluvní stranou kdykoliv označena. To však neplatí

v případě, že by se stala tato informace, k níž se zavazují k povinnosti mlčenlivosti či k povinnosti zachovat důvěrnost informace, podle tohoto ustanovení smlouvy, obecně známou či dostupnou. To se nevztahuje na výstupy z plnění podle této smlouvy. Toto ustanovení platí i po dobu 5 let od ukončení účinnosti této smlouvy, nemá však vliv na případné povinnosti Objednatele vyplývající ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

2. Dodavatel se výslovně zavazuje, že informace získané v souvislosti s plněním předmětu smlouvy nezneužije k jinému účelu než výlučně k plnění této smlouvy.
3. Dodavatel se zavazuje, že neposkytne bez souhlasu Objednatele žádné informace třetím stranám ohledně plnění této smlouvy, včetně informací o konfiguraci SW a HW komponentech datového centra a systému dohledu, které mohl Dodavatel zjistit při implementaci a konfiguraci, nebo jiných prvků, které nejsou součástí plnění této smlouvy. Zároveň se Dodavatel zavazuje, že bude uchovávat citlivé informace ohledně plnění této smlouvy, jako jsou logy, konfigurace a topologie jen po nezbytně nutnou dobu, potřebnou pro řádné a efektivní plnění této smlouvy. Veškeré takové informace je také Dodavatel povinen chránit proti odcizení, či zneužití.
4. Dodavatel se zavazuje, že všechny povinnosti stanovené mu v tomto článku ve stejné podobě uplatní vůči svým zaměstnancům, resp. tyto povinnosti přenesou v rámci svých smluvních vztahů na případné poddodavatele.

Článek VII. Kybernetická bezpečnost

1. Ve vztahu k předmětu plnění Smluvní strany prohlašují, že:
 - a) plnění smlouvy bude probíhat na aktivech představujících soubor technických a programových prostředků, jež jsou významnou a nedílnou součástí více informačních systémů naplňujících definici významného informačního systému (VIS) dle § 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“);
 - b) Objednatel je v pozici správce těchto významných informačních systémů dle § 3 písm. e) ZoKB;
 - c) Dodavatel vystupuje jako významný Dodavatel ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 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 „VoKB“).
2. Dodavatel je povinen v rozsahu plnění dle této smlouvy naplnit všechny kybernetické požadavky a dodržovat tyto po celou dobu trvání této smlouvy (pokud příloha č. 3 této smlouvy nestanoví jinou dobu dodržování kybernetického požadavku).
3. Dodavatel se současně zavazuje poskytovat plnění dle této smlouvy v souladu se ZoKB, VoKB a přílohou č. 3 této smlouvy a s opatřeními, která na jeho základě přijmou k tomu oprávněné orgány veřejné moci, a to včetně opatření, která mají pouze doporučující charakter.
4. Objednatel spadá pod dikci ZoKB a dodané řešení tedy nesmí být v rozporu s požadavky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) pro provoz významných informačních systémů a informačních systémů základních služeb.
5. Dodané řešení musí proto splňovat všechny související požadavky a nařízení a musí umožňovat Objednateli řádné plnění povinností podle ZoKB. V souladu s výše uvedeným je Objednatel povinen podle § 5 VoKB, provádět analýzu rizik a identifikovaná rizika řídit.

Současně je Objednatel povinen se zabývat všemi hrozbami, které prostřednictvím varování vydává NÚKIB, těmito hrozbami se dále zabývat a zohlednit je v analýze rizik.

6. Dodavatel je povinen po celou dobu plnění zajistit dostatečnou bezpečnost jím provozovaných aktiv a souvisejících dat v souladu s platnými obecně závaznými právními předpisy, zejména ZoKB, VoKB a dalšími závaznými akty vydanými ze strany orgánů veřejné moci (NÚKIB či jiného správního orgánu).
7. Dodavatel se zavazuje poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené ZoKB a VoKB. Jestliže Dodavatel při plnění této smlouvy zjistí rozpor postupů Objednatele se ZoKB nebo VoKB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.
8. Smluvní strany v průběhu plnění smlouvy spolu vzájemně komunikují za účelem dosažení požadované úrovně bezpečnosti. V případě ohrožení anebo porušení kybernetické bezpečnosti, zejména v případě výskytu kybernetické bezpečnosti události anebo incidentu, jsou smluvní strany povinny ihned po zjištění takových skutečností hlásit jejich výskyt druhé smluvní straně a společně podnikat potřebné kroky k zajištění obnovení požadované úrovně bezpečnosti.
9. Dle požadavků Objednatele poskytne Dodavatel potřebnou součinnost pro účely testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

Článek VIII. Salvátorské ustanovení

Obě smluvní strany prohlašují, že pokud se kterékoliv ustanovení této smlouvy nebo s ní související ujednání ukáže být neplatným nebo se neplatným stane, že tato skutečnost neovlivní platnost smlouvy jako celku. V takovém případě se obě smluvní strany zavazují nahradit neprodleně neplatné ustanovení ustanovením platným; obdobně se zavazují postupovat v případě ostatních nedostatků smlouvy či souvisejících ujednání.

Článek IX. Trvání a ukončení smlouvy

1. Tato smlouva může být ukončena písemnou dohodou obou smluvních stran.
2. Smluvní strany jsou dále oprávněny od této smlouvy odstoupit v případech stanovených občanským zákoníkem nebo touto smlouvou.
3. Kterákoliv ze smluvních stran může odstoupit od smlouvy v případě, že druhá smluvní strana poruší podstatným nebo neodstranitelným způsobem své povinnosti vyplývající z této smlouvy.
4. Za podstatné porušení smluvních povinností Objednatelem se podle této smlouvy považuje prodlení Objednatele s uhrazením ceny plnění o více než 30 dnů.
5. Za podstatné porušení smlouvy Dodavatelem se považuje:
 - a) nedodržení povinnosti Dodavatele podle čl. VI nebo VII této smlouvy,
 - b) neprovádění plnění podle smlouvy řádně a včas v souladu s pokyny Objednatele nebo v souladu s příslušnými právními předpisy, a to ani v dodatečně stanovené lhůtě 10 pracovních dnů,
 - c) neodstranění vad ve sjednané lhůtě, a to ani v dodatečně stanovené lhůtě 10 pracovních dnů,

- d) dodatečně zjištěný fakt, že údaje uvedené Dodavatelem v rámci předchozího zadávacího řízení nebyly pravdivé.
6. Odstoupení od smlouvy musí být provedeno písemně a doručeno druhé smluvní straně. Právní účinky nastávají okamžikem doručení písemného oznámení o odstoupení od smlouvy druhé smluvní straně, není-li stanoveno jinak.
7. Objednatel je dále oprávněn odstoupit od smlouvy, pokud:
- a) bylo vydáno pravomocné rozhodnutí o úpadku Dodavatele nebo bylo zahájeno insolvenční řízení proti Dodavateli na jeho návrh, nebo v případě, že soud pravomocně rozhodl o zrušení Dodavatele a nařídil jeho likvidaci, nebo Dodavatel přijme rozhodnutí o vstupu do likvidace; nebo
 - b) dojde k významné změně kontroly nad Dodavatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení, nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k plnění smlouvy a tato změna bude Objednatelům vyhodnocena jako bezpečnostní riziko ve smyslu ZoKB.
8. V případě, že tato smlouva zanikne odstoupením, má poskytovatel právo na poměrnou úhradu za část díla již provedeného podle této smlouvy. Toto ustanovení neplatí v případě, že dojde k odstoupení od smlouvy z důvodů na straně Dodavatele.
9. Smluvní strany se dohodly, že v případě ukončení této smlouvy z důvodu uplynutí doby jejího trvání nebo z důvodu jejího ukončení některou ze smluvních stran, a v případě zájmu Objednatel o přechod poskytování všech či některých služeb na třetí osobu, a současně jestliže Objednatel předloží Dodavateli detailní plán přechodu služeb na nového Dodavatele je Dodavatel povinen poskytnout Objednateli a novému Dodavateli součinnost, a to v nezbytně nutném rozsahu a podle plánu přechodu služeb. Dodavatel se zavazuje Objednateli poskytnout rovněž nezbytnou součinnost pro účely vytvoření relevantního plánu přechodu služeb.
10. Smluvní strany se dohodly, že součinnost podle odstavce 10 tohoto článku smlouvy bude Dodavatelem poskytována tak, aby byla minimalizována rizika s přechodem poskytování služeb, a aby byla zajištěna kontinuita poskytování služeb.

Článek X.

Smluvní pokuty, odpovědnost za škody

1. V případě prodlení Objednatel s uhrazením řádně fakturovaných částek podle podmínek stanovených touto smlouvou má Dodavatel nárok na úrok z prodlení v zákonné výši z dlužné částky za každý i započatý den prodlení, nejvýše však v součtu do výše 5 % z fakturované částky.
2. V případě prodlení Dodavatele s plněním této smlouvy uhradí Dodavatel Objednateli smluvní pokutu ve výši 5.000 Kč za každý i započatý den prodlení.
3. V případě porušení své povinnosti ve věci ochrany informací stanovené podle čl. VI této smlouvy uhradí Dodavatel Objednateli smluvní pokutu ve výši 50.000 Kč za každý jednotlivý případ porušení takové povinnosti.
4. V případě porušení své povinnosti ve věci ochrany kybernetické bezpečnosti stanovené podle čl. VII této smlouvy uhradí Dodavatel Objednateli smluvní pokutu ve výši 50.000 Kč za každý jednotlivý případ porušení takové povinnosti.
5. Úrok z prodlení a smluvní pokuta jsou splatné ve lhůtě 10 dnů ode dne doručení písemné výzvy k jejich úhradě.

6. Objednatel nemá právo uplatnit smluvní pokutu, jestliže Dodavatel prokáže, že Objednatel neposkytl Dodavateli spolupůsobení nutné k tomu, aby Dodavatel mohl splnit svůj závazek.
7. Objednatel je oprávněn započítat případné smluvní pokuty oproti ceně za plnění této smlouvy.
8. Zaplacením smluvní pokuty podle této smlouvy není dotčen nárok smluvní strany na náhradu skutečné škody v celém rozsahu způsobené škody. Žádná ze smluvních stran neodpovídá za škodu vzniklou jako následek vyšší moci.

Článek XI. Závěrečná ustanovení

1. Právní vztahy touto smlouvou výslovně neupravené nebo z ní vyplývající se řídí příslušnými ustanoveními občanského zákoníku, příp. zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
2. Smluvní strany bezvýhradně souhlasí s uveřejněním této smlouvy, případných dodatků k této smlouvě, jakož i se zveřejněním dalších aspektů tohoto smluvního vztahu 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. Uveřejnění zajistí Objednatel.
3. Změny a doplnění této smlouvy (s výjimkou změny kontaktních osob dle odstavce 5 tohoto článku smlouvy) lze činit pouze se souhlasem obou smluvních stran písemnou formou, a to prostřednictvím vzestupně číslovaných dodatků, jinak jsou neplatné.
4. Jakékoli oznámení ve smyslu této smlouvy od druhé smluvní strany musí být učiněno písemně.
5. Veškerá komunikace mezi smluvními stranami ve věcech této smlouvy bude probíhat prostřednictvím kontaktních (pověřených) osob, jimiž v dané věci jsou:

a) na straně Objednatele: *(pozn.: bude doplněno před podpisem smlouvy)*

Jméno	E-mail	Telefon	Mobil

b) na straně poskytovatele:

Jméno	E-mail	Telefon	Mobil

6. Smlouva vzniká dnem podpisu oprávněnými zástupci smluvních stran a nabývá účinnosti dnem zveřejnění smlouvy podle zákona o registru smluv.
7. Tato smlouva se vztahuje na právní nástupce smluvních stran.
8. Nedílnou součástí této smlouvy jsou:

Příloha č. 1 – Specifikace předmětu plnění

Příloha č. 2 – Cenová kalkulace

Příloha č. 3 – Specifikace plnění požadavků v oblasti kybernetické bezpečnosti

Příloha č. 4 – Harmonogram dílčích etap.

9. Tato smlouva je vyhotovena v elektronické podobě, kdy bude příslušný dokument opatřen elektronickými podpisy zástupců obou smluvních stran.
10. Obě smluvní strany prohlašují, že se s textem této smlouvy seznámily, obsahu porozuměly, souhlasí s ním a na důkaz toho připojují své podpisy.

V Praze dne

V dne

Objednatel:

Dodavatel:

.....
Ing. Marek Ebert
předseda Rady
Českého telekomunikačního úřadu

.....
.....
.....
.....

Specifikace předmětu plnění

Požadovaná funkcionalita/vlastnost	Nabízené řešení splňuje požadavek (dodavatel doplní ANO/NE)
Platforma	
Nasazení redundantních HW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelérátoru a webového aplikačního firewallu.	
Každé zařízení podporuje připojení 4 x 10/1 Gbps metalické RJ45 porty a alespoň 4x 25/10 Gbps optické SFP+ porty.	
Datová propustnost zařízení alespoň 23 Gbps či více na L4 a 15 Gbps či více na L7	
Minimální propustnost HTTP požadavků: 1,5 mil. za sekundu	
Minimální propustnost L7 požadavků: 800 tis. za sekundu	
Počet současných L4 spojení: min. 17 mil.	
Offload – HW komprese – propustnost min. 10 Gbps	
SSL akcelerace v HW	
Počet SSL transakcí za sekundu min. 10 tis. (při použití 2K klíče)	
Počet SSL transakcí za sekundu min. 8 tis. (při použití ECDSA P-256 klíče)	
Celkový šifrovací výkon min. 8 Gbps	
Nezávislé rozhraní pro management	
Redundantní napájení	
K dispozici jako autonomní box nebo ve formě šasi	
Management: sériový port, GUI, příkazový řádek, iLO	
Operační systém	
Full-Proxy architektura (plné oddělení klientského a serverového spojení)	
Podpora IPv4	
Plná podpora IPv6, IPv4/IPv6 gateway	
Podpora externích šifrovacích karet pro SSL (HSM)	
Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA)	
Podpora Spanning Tree Protokolu (STP)	
Možnost přidat vlastní funkce pomocí skriptování	
Podpora HTTP/2	
Podpora IPsec IKEv2	
Podpora konfigurace a správu zařízení přes REST API	
Podpora SNMP (v1/v2c/v3)	
Možnost aktivovat následující funkce na jedné HW platformě: - L4-7 loadbalancing - ICSA certifikovaný Web aplikační firewall	

Možnost dodatečně aktivovat další funkcionalitu zakoupením licencí:	
- ICSA certifikovaný síťový firewall - Autorizace a autentizace aplikací, SSL VPN - DNS služby a DNS firewall - IP reputační databáze	
Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu	
Podpora Active-Active a Active-Pasive módu	
Možnost vytvoření HA clusteru mezi Virtuální a Hardware platformou	
Web aplikační Firewall	
Integrace s nástrojem na detekci zranitelností webových aplikací	
Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10	
Možnost doprogramovat si filtrovací pravidla pro aplikace	
Automatická korelace zranitelností do jednoho bezpečnostního incidentu	
Ochrana AJAX a JSON aplikací	
Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)	
Podpora Captcha metody	
Automatické odlišení skutečných uživatelů od robotů	
Integrovaný XML firewall	
Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění...	
Automatické nahrávání a aplikování nových signatur	
Podpora pozitivního a negativního bezpečnostního modelu	
Blokování útočníků na základě geolokace	
Podpora ICAP pro antivirovou kontrolu – pro HTTP, SOAP a SMTP	
Ochrana SMTP a FTP na aplikační úrovni	
Podpora SSL (šifrování a dešifrování)	
Podpora různých typů reportů – PCI, geolokační reporty	
Podpora standardů PCI DSS, HIPAA, Basel II a SOX	
Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Oracle Applications, Wordpress a Microsoft SharePoint	
Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. Regionu)	
Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů:	
• Cenzic Hailstorm • WhiteHat Sentinel • IBM Rational AppScan • QualysGuard Web Application Scanning	
Podpora aplikačního firewallu ve virtuálních kontextech	
Podpora aplikačního firewallu v cloudu	

Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu	
Ochrana proti Session Highjacking pomocí Browser Fingerprintingu	
Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávací URL apod.)	
Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace	
Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI	
Podpora a filtrování WebSocket provozu	
Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice	
Možnost ochrany proti Credential Stuffing útokům	
Možnost doplnění modulu pro přístup k online databázi nejnovějších útoků	
Možnost rozšířit DoS ochranu proti přetížení napojením na čističku provozu přes cloud.	
Napojení na globální databázi škodlivých IP adres s automatickým obnovováním a možnost jejich blokování	
Rozpoznání zdrojů Phishingu, Anonymních Proxy a spojení na Command and Control centra Botnetů	
Možnost napojení na CDN	
Schopnost detekovat probíhající útok konkrétní útočné skupiny s cílem zneužít známé zranitelnosti CVE, aktualizace definicí těchto útoků a vytvoření signatur ve WAF v reálném čase.	
Řízení provozu	
Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API	
Podpora REST API	
Autentizace klientů přes LDAP/Radius	
Povolení/zakázání ICMP a ARP pro VIP	
Podpora vysokorychlostního granulórního logování / logování per aplikace / bez omezení výkonnosti zařízení	
Podpora rozvažování zátěže alespoň pro následující metody: - Round Robin - Least Connections - Ratio - Ration Least Connections - Weighted Least Connections	
Podpora filtrace paketů	
Podpora ToS, QoS (marking/preservation/mimic)	
Podpora SNMP (v1/v2c/v3)	
Podpora rozvažování zátěže založené na poměrech (ratio) s perzistencí	
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	
Podpora práce s 4096-bit klíči	
Současná podpora ECC a RSA certifikátu	
Podpora Camellia šifer SSL	

Podpora pro TLS 1.2 a TLS 1.3	
Podpora ECC a DH šifer v HW	
Podpora SSL Forward proxy	
Stavové filtrované paketů (ACL)	
Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb	
Podpora monitorování služeb na základě výkonu konkrétních hostů	
TCP optimalizace síťových toků	
Komprese a cachování specifických služeb	
Podpora zrcadlení SSL relací a SSL spojení v HA clusteru	
Podpora optimalizace dynamické velikosti TLS bloků (TLS record size)	
Řízení přístupu k aplikacím	
Podpora autentizace: - HTTP basic - HTML form - Certificate - OCSP - CRLDP - Radius - LDAP - Active Directory - NTLM v1/v2 - Kerberos - SAML - SecurID - OAM - Tacacs+ - Local DB	
Import uživatelských identit IF-MAP	
Podpora externích přihlašovacích stránek aplikací	
Podpora vysoké dostupnosti AAA serverů	
OTP (generování a ověření)	
Podpora CAPTCHA	
SAML: - SP role - IdP role	
Modifikace SAML atributů	
Podpora SAML 2.0	
Podpora pro vytvoření Single Sign-On (SSO): - HTTP basic - HTML form - NTLM v1/v2 - Kerberos - SAML	
Uchování přihlašovacích údajů v paměti a jejich přeposlání k ověření (User identity credential caching, SSO proxy)	
Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS)	

Podpora Kerberos ticketing	
PCoIP proxy	
RDP proxy	
Patching (maskování) webových portálů: - HTML - JavaScript - CSS - Java	
Podpora uživatelského portálu při publikaci služeb v režimu jednoho URL	
Uživatelský portál, kde se zobrazují aplikace podle přístupových práv	
Podpora L7 ACL	
Podpora importu dynamických ACL z AAA	
Podpora dynamického řízení přístupu	
Podpora zabezpečení vzdálené pracovní plochy vzdáleného uživatele	
Síťová SSL VPN DTLS	
Podpora publikace aplikací formou portálu	
Podpora vzdáleného přístupu k aplikacím bez nutnosti použití tlustého klienta	
Podpora OS: - Windows - MAC - Linux - iOS - Android	
Nativní podpora MDM	
Podpora Oauth 2.0	
Kontrola nastavení zabezpečení koncových bodů (klientů), validace politik, detekce AV a verze, certifikátů aj. parametrů na straně klienta	
Filtrování URL	
URL kategorizační databáze	
Podpora pro vytváření flexibilní a granulární přístupové politiky	
GUI pro vizuální nastavení přístupových bezpečnostních politik a logiky autentizace	
Podpora Microsoft ActiveSync a Outlook Anywhere s klientskou NTLM autentizací	
Zjednodušené řízení přístupové politiky pro VDI technologie Citrix XenApp a XenDesktop	
Podpora „Step-up“ autentizace	

CENOVÁ KALKULACE

	Požadované plnění	Obchodní označení produktu	Cena celkem v Kč bez DPH	Cena celkem v Kč vč. DPH
1.	Dodání 2 kusů appliance zapojených ve vysoké dostupnosti			
2.	SW moduly zajišťující požadované funkce, SW pro centrální management včetně příslušných licencí s platbou za 5 let provozu			
3.	Instalace, konfigurace, zaškolení			
4.	Servisní podpora na 5 let, včetně práce na zaintegrování jednotlivých IS v objemu 150 MD			
5.	5 let RMA podpory 10x5xNBD pro 2 kusy appliance zapojených ve vysoké dostupnosti			
Celkem				

Specifikace plnění požadavků v oblasti kybernetické bezpečnosti

Vymezení pojmů

Pro potřeby této přílohy smlouvy jsou použity následující zkratky a pojmy:

ZoKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

VoKB – 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) v platném znění

Kybernetické požadavky – kybernetickými požadavky se rozumí všechny bezpečnostní požadavky ve smyslu ZoKB a VoKB,

Produkční prostředí – produkčním prostředím se rozumí prostředí běžně přístupné uživatelům IS ČTÚ v ostrém provozu,

Testovací prostředí – prostředí určené k provádění testů, vzdělávání uživatelů apod, a to v podobě, nastavení a rozsahu umožňujícím účinně zkoumat funkcionality testovacích verzí IS ČTÚ,

Prostředí objednatele – fyzický perimetr určený ohraničením fyzického prostoru v nájmu nebo majetku objednatele anebo logický perimetr definovaný hraničními síťovými prvky ve správě nebo majetku objednatele,

Osoba na straně dodavatele – fyzická osoba podílející se na poskytování předmětu plnění a mající pracovněprávní či obdobný smluvní vztah s dodavatelem nebo jeho poddodavateli,

Osobní údaje – každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů), jestliže lze subjekt údajů přímo či nepřímo pomocí tohoto údaje identifikovat,

Zpracování osobních údajů – jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

1. ÚVODNÍ USTANOVENÍ

- 1.1 Z důvodu nutnosti plnění povinností stanovených objednateli jakožto povinné osobě ve smyslu VoKB je dodavatel povinen nad rámec povinností stanovených smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této přílohy č. 9 smlouvy. Účelem této přílohy č. 9 smlouvy tak je dodržet povinnost objednatele dle § 4 odst. 4 ZoKB zahrnout požadavky vyplývající z bezpečnostních opatření do smluvního ujednání s dodavatelem.

2. SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

- 2.1 Dodavatel je povinen se v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 3 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:
- a) Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně dodavatele při poskytování předmětu plnění dle smlouvy.
 - b) Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
 - c) Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy objednateli zpřístupnit.
 - d) Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně dodavatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
- 2.2 Dodavatel je dále povinen dodržovat bezpečnostní politiku objednatele, byl-li s ní prokazatelně seznámen.

3. ŘÍZENÍ AKTIV

- 3.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 4 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této smlouvy (aktivity se rozumí např. data a informace k předmětu plnění dle této smlouvy, systémy ICT, moduly, hardware prvky – infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení apod.), a tato aktiva strukturovaně popsat a objednateli předložit následně na vyžádání, a to po celou dobu trvání smlouvy.

4. ŘÍZENÍ RIZIK

- 4.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 5 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

- a) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění dle smlouvy.
- b) V minimálním intervalu jednou ročně (nebo i v případě významných změn činností prováděných pro objednatele nebo změn spravovaných aktiv) vytvořit a bude-li to objednatel požadovat, předložit mu zprávu o hodnocení rizik, která bude minimálně pokrývat:
 - i) Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;
 - ii) Identifikaci a hodnocení rizik s vazbou na předmět plnění;
 - iii) Realizovaná bezpečnostní opatření;
 - iv) Nepokrytá bezpečnostní rizika a návrh opatření;
 - v) Vyhodnocení bezpečnostních událostí a incidentů;
 - vi) Aktuální stav souladu dodavatele s kybernetickými požadavky včetně přehledu kybernetických požadavků, které:
 - nebyly aplikovány, včetně odůvodnění, a
 - byly aplikovány, včetně způsobu plnění.

5. ORGANIZAČNÍ BEZPEČNOST

- 5.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 6 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:
- a) Jmenovat nejpozději do 30 dnů po uzavření smlouvy odpovědnou kontaktní osobu/y pro potřeby zajištění plnění kybernetických požadavků a související komunikace mezi smluvními stranami (dále jen „kontaktní osoba pro kybernetickou bezpečnost“). Kontaktní osobu/y pro kybernetickou bezpečnost sdělí dodavatel písemně objednateli v téže lhůtě.
 - b) Využívat pro poskytování předmětu plnění dle smlouvy pouze oprávněných osob, které byly řádně seznámeny s příslušnými ustanoveními interních předpisů objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění dle smlouvy a stanovit bezpečnostní role těchto oprávněných osob s jasně definovanými odpovědnostmi a pravomocemi.

6. ŘÍZENÍ DODAVATELŮ

- 6.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 8 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:
- a) Využívá-li při poskytování předmětu plnění dle smlouvy subdodavatele, zajistit v obdobném rozsahu dodržování kybernetických požadavků rovněž ve smluvních vztazích se svými subdodavateli.
 - b) Dodržovat podmínky při zpracování osobních údajů pro zapojení každého dalšího dodavatele.

7. BEZPEČNOST LIDSKÝCH ZDROJŮ

7.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 9 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

- a) Zajistit, aby kontaktní osoba pro kybernetickou bezpečnost nejpozději do 60 dnů od uzavření smlouvy potvrdila písemně objednateli, že všechny osoby podílející se na poskytování předmětu plnění dle smlouvy za dodavatele byly prokazatelně seznámeny s těmito kybernetickými požadavky a příslušnými ustanoveními interních předpisů objednatele.
- b) Dodržovat příslušná ustanovení interních předpisů objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje:
 - i) školení pracovníků dodavatele zajištěné objednatelem
 - ii) protokolární či elektronické předání příslušných předpisů nebo
 - iii) objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní předpisy, jejichž konkrétní jmenovitý seznam bude dodavateli – současně s poskytnutím přístupu – protokolárně předán.
- c) Při provádění dohledu nad předmětem plnění dle smlouvy, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění dle smlouvy.
- d) Zajistit, aby osoby podílející se na poskytování plnění objednateli v prostředí/nebo s prostředky objednatele:
 - i) pro uložení a sdílení dat a informací objednatele využívaly pouze k tomu schválené prostředky (aktiva);
 - ii) neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující dobré jméno objednatele;
 - iii) nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo předpisy upravující ochranu duševního vlastnictví;
 - iv) nenavštěvovaly internetové stránky s eticky nevhodným obsahem;
 - v) nerealizovaly pokusy o neautorizovaný přístup ke zdrojům objednatele ani ke zdrojům jiných subjektů;
 - vi) nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků objednatele, a to ani v případě, kdy jim byl prostředek objednatele svěřen do správy;
 - vii) nepodílely se s prostředky objednatele na šíření spamu ani škodlivého softwaru,

a to i tehdy, pokud jsou prostředky objednatele používány mimo jeho prostředí.

7.2 Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivitám objednatele je na straně objednatele zpracování osobních údajů pověřených osob dodavatele, které se podílejí na poskytování plnění dle smlouvy. Pokud nebude objednateli umožněno osobní údaje pověřených osob dodavatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům objednatele.

7.3 Dodavatel je dále povinen:

- a) Prohlubovat znalostí osob podílejících se na poskytování plnění objednateli v oblasti bezpečnosti informací.
- b) Stanovit práva a povinnosti osob podílejících se na poskytování plnění objednateli v oblasti bezpečnosti informací.

8. ŘÍZENÍ PROVOZU A KOMUNIKACÍ

8.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 10 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

- a) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění dle smlouvy.
- b) Na vyžádání ve lhůtě, která nebude kratší než 10 pracovních dnů, poskytnout objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.
- c) Zajistit, že pro poskytování předmětu plnění dle smlouvy budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou legislativou, a to především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví (zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů).

8.2 Dodavatel je dále povinen provést a zabezpečit dodržování následujících opatření:

- a) Implementaci procesů pro řízení ICT (tj. řízení incidentů, řízení změn, řízení životního cyklu systémů apod.).
- b) Zavedení postupů pro ochranu proti škodlivému kódu včetně řízení technických zranitelností v informačním systému, který je využíván k poskytování předmětu plnění dle smlouvy.
- c) Zavedení pravidel a postupů pro ochranu informací a dat.
- d) Stanovení pracovních postupů pro instalaci, spouštění, ukončování provozu technických aktiv a pracovní postupy pro řešení mimořádných stavů.
- e) Řízení přístupu k datům a systémům, které spadají do rozsahu poskytování předmětu plnění dle smlouvy.

9. ŘÍZENÍ ZMĚN

9.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 11 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:

- a) Přiměřeně reagovat na změny v oblasti kybernetické bezpečnosti na straně objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.
- b) Aktivně spolupracovat při testování významné změny v oblasti kybernetické bezpečnosti na straně objednatele.

10. ŘÍZENÍ PŘÍSTUPU

- 10.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 12 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:
- a) Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům objednatele.
 - b) Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu dodavatele. V opačném případě musí dodavatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit objednateli kdykoli v průběhu trvání účinnosti této smlouvy a tři měsíce po jejím ukončení, ve lhůtě, která nebude kratší než 6 pracovních dnů.
 - c) Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou, 1 rok, 1 měsíc apod).
 - d) Zajistit, aby osoby podílející se na poskytování předmětu plnění dle smlouvy a mající přístup k informačním aktivům objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.
 - e) Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně dodavatele, které přistupují do prostředí objednatele.
- 10.2 Dodavatel bere na vědomí, že oprávnění přístupu k systémům ICT objednatele je možné povolit pouze fyzické identitě zaměstnance dodavatele/subdodavatele, a to na základě příslušného požadavku dodavatele.
- 10.3 Dodavatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.
- 10.4 Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet objednatelem zablokován a řešen jako bezpečnostní incident a dále mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům objednatele).

11. AKVIZICE, VÝVOJ A ÚDRŽBA

- 11.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 13 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:
- a) Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, pokud jsou předmětem plnění dle smlouvy či jeho součástí.
 - b) Není-li smlouvou stanoveno jinak, předat při ukončení smlouvy objednateli kompletní provozní a bezpečnostní dokumentaci předmětu plnění dle smlouvy. Ta musí být předána minimálně v následujícím rozsahu:

- i) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
- ii) dokumentaci obsahující popis autorizačního konceptu a oprávnění;
- iii) dokumentaci obsahující instalační a konfigurační postupy;

Výše uvedenou dokumentaci dodavatel předá objednateli v přiměřené lhůtě, nejpozději pak dle předchozí dohody smluvních stran.

11.2 V případě, že předmět plnění dle smlouvy zahrnuje částečně i vývoj softwaru, je dodavatel povinen:

- a) Dodržovat a implementovat obecně uznávané „nejlepší praktiky“ pro bezpečný vývoj softwaru. Základním pravidlem zde je myslet na bezpečnost softwaru ve všech jeho vývojových fázích.
- b) Na vyžádání alespoň 6 pracovních dnů předem umožnit objednateli audit prováděného nebo provedeného plnění a na písemnou žádost objednatele předložit ve stanovené lhůtě vyvíjený zdrojový kód na provedení tzv. codereview, a to především za účelem ověření skutečnosti, zda dodavatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito bezpečnostními požadavky.
- c) Poskytovat objednateli v termínech stanovených objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru (nejdříve však od zahájení testovacího provozu) či kdykoli po jeho předání.
- d) Pokud je součástí plnění dle smlouvy i instalace operačního systému, případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v testovacím prostředí či produkčním prostředí objednatele.
- e) Zajistit bezpečnost testovacího prostředí u dodavatele a ochranu poskytnutých testovacích dat objednatelem.
- f) Zajistit, že v rámci poskytovaného plnění bude dodáváný software
 - i) v souladu s bezpečnostními politikami a standardy objednatele;
 - ii) otestován na soulad s bezpečnostními politikami objednatele, pokud byl s takovými bezpečnostními politikami prokazatelně seznámen.
- g) Instalovat software pouze na základě předem schválených migračních postupů objednatelem.
- h) Předat zdrojový kód objednateli bezpečnou formou zajišťující jeho integritu.
- i) Zajistit řízení verzí zdrojového kódu, jeho zálohování a jeho uložení mimo produkční prostředí.

12. ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

12.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 14 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy:

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

- b) Bez zbytečného odkladu hlásit objednateli všechny kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty s potenciálním negativním dopadem na objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím kontaktní osoby pro kybernetickou bezpečnost.
 - c) Vyhodnocovat informace o kybernetických bezpečnostních incidentech a uchovávat je pro budoucí použití, a to s ohledem na požadavky použitelné platné a účinné legislativy.
 - d) V případě vzniku kybernetické bezpečnostní události a následného zvládání a vyhodnocování možného kybernetického bezpečnostního incidentu a/nebo v případě podezření na možný kybernetický bezpečnostní incident poskytnout objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či podezřelém jednání osob na straně dodavatele.
 - e) Spolupracovat při analýze příčin kybernetického bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Zhotovitel kybernetický bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
 - f) Po dohodě s objednatelem realizovat bez zbytečného odkladu opatření požadovaná objednatelem ke snížení dopadu kybernetického bezpečnostního incidentu nebo zamezení pokračování kybernetického bezpečnostního incidentu, nejpozději pak v termínech prokazatelně stanovených objednatelem.
- 12.2 Dodavatel bere na vědomí, že postup zvládání kybernetického bezpečnostního incidentu či jiný důsledek porušení bezpečnostních požadavků, jehož příčina je na straně dodavatele, nebude posuzován 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 ve smlouvě nejsou tímto ustanovením dotčena.

13. ŘÍZENÍ KONTINUITY ČINNOSTÍ

- 13.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 15 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:
- a) Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění dle smlouvy.
 - b) Pravidelně kontrolovat a testovat, že je schopen kontinuitu těchto aktiv zajistit dle sjednané SLA.

14. KONTROLA A AUDIT

- 14.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy poskytnout adekvátní součinnost při výkonu kontroly objednatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle § 23 ZoKB.
- 14.2 Dodavatel umožní objednateli alespoň jednou ročně po dobu účinnosti smlouvy provedení auditu kybernetické bezpečnosti (dále jen audit) u dodavatele a jeho případných subdodavatelů:

- a) jehož rozsah bude ohraničen v rámci ICT prostředků dodavatele používaných pro potřeby plnění smlouvy a uloženými či zpracovávanými daty a informacemi objednatele v ICT prostředí dodavatele a
 - b) jehož předmětem bude naplnění kybernetických požadavků a vyhodnocení rizik dle bodu 4 této přílohy smlouvy.
- 14.3 Objednatel je oprávněn při provedení auditu využít třetí stranu. V případě využití třetí strany bude objednatel odpovídat za třetí stranu, jako by audit kybernetické bezpečnosti prováděl sám, včetně odpovědnosti za případnou způsobenou újmu.
- 14.4 Dodavatel umožní objednateli audit provedený prostředky objednatele nebo třetí strany, a to v lokalitě dodavatele i vzdáleně, pokud to technické prostředky dodavatele umožňují.
- 14.5 Dodavatel je povinen nedostatky zjištěné:
- a) na základě provedení hodnocení rizik dle bodu 4 této přílohy smlouvy, nebo
 - b) v rámci auditu kybernetické bezpečnosti dle bodu 14.2 této přílohy smlouvy
- odstranit ve lhůtě určené v písemném oznámení objednatele, která nebude kratší než 20 pracovních dnů. Nestanoví-li objednatel lhůtu v písemném oznámení, zavazují se smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevyší 60 dnů.
- 14.6 Dodavatel je dále povinen:
- a) Poskytnout na vyžádání objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění kybernetických požadavků.
 - b) Na požádání s objednatelem konzultovat kdykoli v průběhu realizace plnění dle smlouvy detailní nastavení bezpečnostních opatření k naplnění kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků.
 - c) Neprodleně informovat objednatele o všech významných změnách v naplnění kybernetických požadavků, které nastanou kdykoli v průběhu trvání smlouvy.
 - d) Bezodkladně a s vyvinutím maximálního úsilí zajistit náhradní způsob naplnění kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní.
 - e) Při výkonu své činnosti včas a prokazatelně upozornit objednatele na případnou zřejmou nevhodnost jeho příkazů či doporučení, vztahujících se ke kybernetickým požadavkům, jejichž následkem může vzniknout případná újma anebo nesoulad s příslušnými zákony nebo jinými obecně závaznými právními předpisy.

15. TECHNICKÁ OPATŘENÍ

- 15.1 Dodavatel se bude v rozsahu předmětu plnění dle smlouvy aktivně podílet na splnění povinností uvedených v § 17 až § 27 VoKB, které musí splnit objednatel. Minimálně se dodavatel zavazuje v rozsahu předmětu plnění dle smlouvy na své straně:
- a) Dodržovat příslušné interní předpisy objednatele, s nimiž byl prokazatelně seznámen, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěna aktiva systémů ICT, anebo datové nosiče.
 - b) V rozsahu předmětu plnění dle smlouvy zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv objednatele, pokud s ní byl dodavatel seznámen.

- c) Realizovat bezpečnostní opatření pro odstranění nebo blokování komunikačních spojení, která neodpovídají požadavkům na ochranu integrity a bezpečnosti komunikační sítě.
- d) Realizovat přístupy z mobilních zařízení k aktivům v produkčním i testovacím prostředí objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).
- e) Připojovat do produkčního prostředí objednatele pouze ta síťová zařízení (switch, wifi router apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně objednatele.
- f) Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, pakliže tento je součástí sjednaného rozsahu předmětu plnění dle smlouvy a je současně ve správě dodavatele.
- g) Na aktiva objednatele bez jeho písemného souhlasu neinstalovat a nepoužívat v prostředí objednatele následující typy nástrojů, pokud vysloveně nejsou součástí předmětu plnění dle smlouvy:
 - i) Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
 - ii) Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.
 - iii) Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.
 - iv) Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejít schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do počítačového systému.
 - v) Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje stávající bezpečnostní opatření v prostředí Objednatele.
- h) Připojovat do prostředí objednatele pouze zařízení ICT, která splňují následující požadavky:
 - i) jsou příslušným způsobem zabezpečena a chráněna proti malware a jinému škodlivému softwaru – minimálně instalovaný a aktivní antivir s aktuální definiční sadou, pokud možno instalované veškeré doporučené bezpečnostní záplaty pro OS a používaný SW, správně nakonfigurovaný a aktivní firewall;
 - ii) způsob jejich připojení je definován v příslušné provozní nebo projektové dokumentaci nebo je v souladu s příslušnými interními předpisy objednatele.
- i) Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.
- j) Na vyžádání poskytnout objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění dle smlouvy, a to po celou dobu trvání smlouvy a pak po dobu 2 let po jejím ukončení.
- k) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění dle smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

- l) Pro veškeré on-line transakce realizované prostřednictvím webových technologií implementovat doporučené a schválené TLS/SSL certifikáty s cílem zajistit důvěrnost a integritu komunikace protistran.
 - m) Veškeré neveřejné informace poskytnuté objednatelem a ukládané na mobilní zařízení anebo přenosná paměťová média, která jsou ve správě dodavatele, chránit vhodným šifrováním a proti neautorizovanému přístupu.
- 15.2 Dodavatel bere na vědomí, že v případě, kdy technické spojení ze strany dodavatele narušuje bezpečný chod ostatních služeb objednatele, může být toto spojení ze strany objednatele bez předchozího upozornění ihned ukončeno.
- 15.3 Dodavatel bere na vědomí, že veškeré jeho aktivity a jeho plnění realizované v prostředí objednatele mohou být monitorovány a vyhodnocovány v rozsahu předmětu plnění smlouvy a v souladu s příslušnými interními dokumenty objednatele.

Harmonogram dílčích etap

Pořadí aktivit	Název aktivity	Nejzazší termín plnění
1	Nabytí účinnosti smlouvy	T0
2	Zpracování projektové dokumentace	T0 + 23 PD
3	Přípravné práce a příprava HW, fyzická instalace zařízení	T0 + 35 PD
4	Základní konfigurace včetně instalace SW a potřebných licencí, v případě potřeby implementace příslušných HW/SW update od výrobce	T0 + 35 PD
5	Rozšířená konfigurace jednotlivých komponent a nasazení příslušných politik web aplikačního firewallu ve spolupráci s Objednatelem	T0 + 38 PD
6	Dokumentace skutečného provedení, zaškolení obsluhy	T0 + 42 PD
7	Ukončení akceptačního řízení	T0 + 46 PD

PD – pracovní den

Vzor čestného prohlášení
(základní způsobilost)

Dodavatel, se sídlem, IČO: podávající nabídku k nadlimitní veřejné zakázce na dodávky a služby s názvem „Dodávka loadbalanceru a aplikačního firewallu“ tímto prohlašuje, že splňuje základní způsobilost podle bodu 8.5 zadávací dokumentace, tj. že:

- a) nebyl v zemi svého sídla v posledních 5 letech před zahájením výběrového řízení pravomocně odsouzen pro trestný čin uvedený v příloze č. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, nebo obdobný trestný čin podle právního řádu země sídla dodavatele; k zahlazeným odsouzením se nepřihlíží,
- b) nemá v České republice nebo v zemích svého sídla v evidenci daní zachycen splatný daňový nedoplatek,
- c) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na veřejné zdravotní pojištění,
- d) nemá v České republice nebo v zemi svého sídla splatný nedoplatek na pojistném nebo na penále na sociálním zabezpečení a příspěvku na státní politiku zaměstnanosti, a který
- e) není v likvidaci, proti němuž nebylo vydáno rozhodnutí o úpadku, vůči němuž nebyla nařízena nucená správa podle jiného právního předpisu nebo není v obdobné situaci podle právního řádu země sídla dodavatele.

Dodavatel dále čestně prohlašuje, že podmínku podle § 74 odst. 1 písm. a) ZZVZ splňuje zároveň každý člen jeho statutárního orgánu, přičemž je-li členem statutárního orgánu dodavatele právnická osoba, splňuje tuto podmínku tato právnická osoba, každý člen statutárního orgánu této právnické osoby a osoba zastupující tuto právnickou osobu v statutárním orgánu dodavatele.

V dne

.....
Jméno a podpis osoby oprávněné zastupovat dodavatele

Seznam významných dodávek/služeb

Dodavatel:

Jméno / název / obchodní firma:	
Bydliště / sídlo / místo podnikání:	
Právní forma:	
IČO:	

Dodavatel níže předkládá seznam významných dodávek/služeb realizovaných dodavatelem za poslední 3 roky před zahájením zadávacího řízení, včetně uvedení požadovaných údajů:

- a) název zakázky,
- b) název a identifikační údaje subjektu vč. sídla, kterému byla významná dodávka/služba poskytnuta,
- c) popis dodávky/služby, ze kterého budou požadavky zadavatele na významné dodávky/služby vyplývat,
- d) informaci o období realizace významné dodávky/služby od–do v měsících/rocích (např. leden 2022–září 2023),
- e) hodnotu významné dodávky/služby v Kč bez DPH,
- f) jméno a kontaktní údaje osoby objednatele, u které si bude moci zadavatel případně ověřit předložené informace.

Významná dodávka/služba č. 1	
Název zakázky	
Objednatel	
název / obchodní firma	
právní forma	
adresa sídla	
adresa poskytnutí	
IČO	
Popis dodávky/služby	
Doba realizace (od–do)	
Cena (v Kč bez DPH)	
Kontaktní osoba objednatele (pro ověření reference)	
jméno a příjmení	
funkce nebo pracovní zařazení	
telefonní číslo	
e-mail	

Významná dodávka/služba č. 2	
Název zakázky	
Objednatel	
název / obchodní firma	
právní forma	
adresa sídla	
adresa poskytnutí	
IČO	
Popis dodávky/služby	
Doba realizace (od–do)	
Cena (v Kč bez DPH)	
Kontaktní osoba objednatele (pro ověření reference)	
jméno a příjmení	
funkce nebo pracovní zařazení	
telefonní číslo	
e-mail	

V dne

.....

Jméno a podpis osoby oprávněné zastupovat dodavatele

Informace o zajištění kybernetické bezpečnosti dodavatele a poddodavatelů

Postup vyplnění:

1. Dodavatel odpoví na **VŠECHNY** otázky v SEKCI A - F.
2. Dodavatel a poddodavatelé vyplňují každý vlastní tabulku podle stavu bezpečnosti jejich vlastního prostředí.

Zbývá vyplnit 49 otázek.

SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY		49
1	Které standardy a nejlepší praktiky na své informační systémy organizace dodavatele aplikuje:	
a.	ISO 9001	
b.	ISO/IEC 27001	
c.	ISO 22301, BS 25999	
d.	ISO/IEC 20000-1, ITIL, CobIT	
SEKCE B – ZÁKLADNÍ OPATŘENÍ		
2	Má organizace dodavatele manažera bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností?	
3	Byl v organizaci v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti informační bezpečnosti?	
4	Bylo v organizaci v posledních 12ti měsících provedeno hodnocení rizik v oblasti informační bezpečnosti?	
5	Které oblasti pokrývá dokument bezpečnostní politiky, pokud v organizaci dodavatele existuje?	
a.	Procesy řízení rizik	
b.	Klasifikace aktiv	
c.	Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti	
d.	Ochrana osobních dat	
e.	Identifikace a autentizace uživatelů	
f.	Přístup k datům na základě rolí (RBAC, Role Based Access Control)	
g.	Řízení privilegovaných přístupů	
h.	Ochrana koncových stanic	
i.	Ochrana mobilních zařízení a vzdáleného přístupu	
j.	Ochrana emailu a vnitrofiremní komunikace (instant messaging)	
k.	Ochrana přístupu do internetu	
l.	Ochrana médií	
m.	Procesy řízení změn	
n.	Ochrana bezdrátových sítí a komunikace	
o.	Fyzická bezpečnost informačních aktiv	
p.	Bezpečnostní školení koncových uživatelů a administrátorů	
q.	Ochrana proti škodlivému softwaru	
r.	Ochrana při výměně dat	
s.	Procesy zvládání kybernetických incidentů	
t.	Procesy řízení rizik dodavatelů	
u.	Bezpečnost lidských zdrojů	
v.	Bezpečnostní audity a analýzy	
w.	Řízení kontinuity činnosti a havarijní plánování	
SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE		
6	Které níže uvedené bezpečnostní technologie organizace dodavatele provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?	
a.	Antivirový software na pracovních stanicích	
b.	Antivirový software na mobilních zařízeních	
c.	Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)	
d.	Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Privileged Identity/Access Management)	
e.	Více-faktorová autentizace	
f.	Automatizovaný nástroj pro řízení technologických zranitelností	
g.	Nástroj pro řízení přístupu k síti (NAC, Network Access Control)	
h.	Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service)	
i.	Šifrovací nástroje a techniky	
j.	Firewall	
k.	Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Information and Event Management)	
7	Byly interní systémy organizace dodavatele v posledních 12ti měsících podrobeny penetračnímu testování?	
SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ		
8	Má organizace dodavatele zaveden proces zvládání bezpečnostních incidentů?	
9	Jsou všichni zaměstnanci organizace dodavatele pravidelně (min. 1x za 24 měsíců) vzdělávání v identifikaci bezpečnostních incidentů?	
SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ		
10	Má organizace dodavatele zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance?	
11	Jsou noví zaměstnanci organizace dodavatele vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům?	
12	Dokumentuje organizace dodavatele účast pracovníků na bezpečnostních školeních a vzdělávacích programech?	
13	Vyžaduje organizace dodavatele po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	
14	Vyžaduje organizace dodavatele po zaměstnancích podepsání etického kodexu?	

Zbývá vyplnit 49 otázek.

SEKCE F - DALŠÍ OTÁZKY		
101	Je organizace dodavatele orgánem nebo osobou povinnou dle § 3 zákona č. 181/2014 Sb.?	
102	Má organizace dodavatele zaveden certifikovaný systém řízení dle ISO/IEC 27001:2005?	
103	Jsou dodavatelé organizace dodavatele vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům?	
104	Vyžaduje organizace dodavatele po pracovnících dodavatele s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	
105	Jaké negativní dopady pocítila organizace dodavatele v souvislosti s kybernetickým incidentem, pokud v minulosti nastal:	
a.	Výpadek sítě	
b.	Nedostupnost emailu a kancelářských aplikací	
c.	Neoprávněné zneužití identity	
d.	Prozrazení chráněných dat	
e.	Ztráta nebo zničení dat	
f.	Finanční ztráta	
g.	Ztráta duševního vlastnictví	
h.	Poškození pověsti organizace dodavatele	
i.	Negativní publicita v médiích	
j.	Ztráta hodnoty organizace dodavatele	
k.	Trestní stíhání organizace dodavatele	