evidenční číslo smlouvy ŘLP ČR, s.p.:062/2015/PS/D2
evidenční číslo smlouvy poskytovatele.:

818/2020/RLPCR

Řízení letového provozu
České republiky

Dodatek č. 2 k servisní smlouvě na poskytování servisní podpory ATM systémů

uzavřené podle § 1746 odst. 2 zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
(dále jen „**občanský zákoník**“)

(dále jen „**dodatek**“)

1. Smluvní strany

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)
se sídlem: Navigační 787, 252 61 Jeneč
zastoupený: Ing. Janem Klasem, generálním ředitelem
IČO: 497 10 371
DIČ: CZ699004742
bankovní spojení: ČSOB Praha 5, č. účtu 88153/0300
SWIFT kód: CEKOCZPP
zapsaný v obchodním rejstříku vedeném Městským soudem v Praze v oddíle A, vložce 10771,

(dále jen „**objednatel**")

a

CS SOFT a.s.
se sídlem: K Letišti 6/1019, 160 08 Praha 6
zastoupený: Ing. Aleš Klepek, předseda představenstva
Ing. Zdeněk Dvořák, člen představenstva
IČO: 257 81 723
DIČ: CZ25781723
bankovní spojení: [redacted]
zapsaný v obchodním rejstříku vedeném u Městského soudu v Praze, v oddíle B, vložce 15253

(dále jen „**poskytovatel**“)

(objednatel a poskytovatel rovněž jako „**smluvní strany**“).

2. Preambule

2.1 Smluvní strany uzavřely dne 30.6.2015 servisní smlouvu na poskytování servisní podpory ATM systémů (číslo smlouvy ŘLP ČR, s.p.: 062/2015/PS/033), ve znění dodatku č. 1 ze dne 1.11.2018 (dále jen „**smlouva**“).

2.2 Vzhledem k tomu, že poskytovatel byl vyhodnocen jako významný dodavatel ve smyslu § 2, písm. n) vyhlášky č. 82/2018 Sb. ze dne 21. května 2018, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), uzavírají smluvní strany tento dodatek, kterým do smlouvy formou přílohy ke smlouvě implementují požadavky přílohy č. 7 vyhlášky o kybernetické bezpečnosti).

3. Předmět dodatku

3.1 S ohledem na skutečnosti uvedené v odst. 2.2 tohoto dodatku se smluvní strany dohodly, že nedílnou součástí smlouvy se stává příloha č. 1 tohoto dodatku, která obsahuje požadavky přílohy č. 7 vyhlášky o kybernetické bezpečnosti (tj. informace týkající se bezpečnostních opatření pro smluvní vztahy s významnými dodavateli), přičemž zmíněná příloha č. 1 tohoto dodatku tvoří přílohu č. 9 smlouvy.

4. Závěrečná ustanovení dodatku

4.1 Ostatní ustanovení smlouvy zůstávají v platnosti beze změn.

4.2 **Tento dodatek se uzavírá elektronicky, a to pouze v jednom elektronickém vyhotovení.**

4.3 Tento dodatek nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem jeho uveřejnění v registru smluv.

4.4 Uveřejnění. Poskytovatel bere na vědomí, že objednatel je povinen uveřejnit tento dodatek v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a registru smluv (zákon o registru smluv) ve znění pozdějších předpisů. Při uveřejnění tohoto dodatku v registru smluv bude znečitelněno: bankovní spojení poskytovatele v čl. 1 dodatku, podpisy na dodatku, kontakty v příloze č. 1 dodatku a odst. 8.5 přílohy č. 1 dodatku.

4.5 Nedílnou součástí tohoto dodatku je následující příloha:

Příloha č. 1 tvořící přílohu č. 9 smlouvy – „Bezpečností opatření pro smluvní vztahy s významnými dodavateli dle přílohy č. 7 vyhlášky č. 82/2018 Sb. bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“

.....[redacted].....

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)

[redacted]

.....

Ing. Aleš Klepek

Předseda představenstva

CS SOFT a.s.

[redacted]

.....

Ing. Zdeněk Dvořák

Člen představenstva

CS SOFT a.s.

Příloha č.1 dodatku č. 2 servisní smlouvy číslo 062/2015/PS/033 na poskytování servisní podpory ATM systémů (dále též „smlouva“) k zajištění opatření v oblasti informační a kybernetické bezpečnosti

„Smluvní zajištění opatření v oblasti informační a kybernetické bezpečnosti ve smyslu § 8, odst. 2 vyhlášky č 82/2018 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů“

1. Preambule

1.1 Smluvní partner bere na vědomí, že je významným dodavatelem dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti pro objednatele Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.), který je správcem informačních a komunikačních systémů kritické informační infrastruktury. Dodavatelem se pro účely této přílohy dodatku smlouvy rozumí společnost CS SOFT a.s. Objednatelem se pro účely této přílohy dodatku smlouvy rozumí ŘLP ČR, s.p.

1.2 [redacted]

1.3 Dodavatel se zavazuje dodržovat požadavky systému řízení bezpečnosti informací uvedené v tomto dodatku, smlouvě a bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.

1.4 Plnění dále uvedených bezpečnostních pravidel vyžaduje objednatel ve vztahu ke všem informačním / komunikačním systémům uvedeným v čl. 1.2 této přílohy dodatku smlouvy. U ostatních podporovaných systémů je dodržování bezpečnostních pravidel vyžadováno přiměřeným způsobem v souladu s nejlepší praxí informační bezpečnosti.

1.5 Pokud je některé z ustanovení smlouvy a jejích příloh v konfliktu s ustanoveními této přílohy dodatku smlouvy nebo bezpečnostními pravidly distribuovanými v souladu s čl. 6 této přílohy dodatku smlouvy, postupují smluvní strany v souladu s ustanoveními později uzavřeného ujednání.

2. Definice pojmů

2.1 „Aktivem“ se rozumí souhrn informací a služeb, které jsou nezbytné pro provozování informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

2.2 „Bezpečnostním incidentem“ se rozumí narušení bezpečnosti informací v informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

2.3 „Bezpečnostním opatřením“ je úkon, jehož cílem je zajištění bezpečnosti informací v informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy, jeho dostupnosti a spolehlivosti v kybernetickém prostoru.

2.4 „Bezpečnostní politikou“ je soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.

2.5 „Bezpečnostní událostí“ taková událost, která může způsobit narušení bezpečnosti informací v informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

2.6 „Dodavatelem“ významný dodavatel dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti.

2.7 „Kritickou informační infrastrukturou“ prvek nebo systém prvků nezbytných pro provozování informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy.

2.1 „Subdodavatelem“ – dodavatel, který poskytuje služby nebo výrobky dodavateli. Přitom musí jít o produkty nezbytné pro zajištění bezpečnosti informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy. Nejedná se o dodavatele standardního softwarového nebo hardwarového řešení (COTS) nebo telekomunikačních služeb.

3. Bezpečnost informací

3.1 Dodavatel je povinen zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy a vést o nich bezpečnostní dokumentaci.

3.2 Východiskem pro nastavení bezpečnostních opatření jsou požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, vyhlášky o kybernetické bezpečnosti, případně normy ČSN ISO/IEC 27001.

3.3 Provádění bezpečnostních opatření u dodavatele ověřuje objednatel postupem dle čl. 15 této přílohy nebo platným certifikátem ISO/IEC 27001, případně jiným zavedeným a platným mezinárodně uznávaným systémem řízení bezpečnosti informací u dodavatele.

3.4 Dodavatel provádí opatření k zajištění důvěrnosti dat souvisejících s poskytováním servisní podpory informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy v souladu s požadavky čl. 11 a čl. 13 smlouvy a bezpečnostními pravidly distribuovanými v souladu s čl. 6 této přílohy dodatku smlouvy.

3.5 Dodavatel provádí opatření k zajištění integrity dat souvisejících s poskytováním servisní podpory informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy v souladu s bezpečnostními pravidly distribuovanými v souladu s čl. 6 této přílohy dodatku smlouvy.

3.6 Dodavatel provádí opatření k zajištění dostupnosti dat souvisejících s poskytováním servisní podpory informačních / komunikačních systémů uvedených v čl. 1.2 této přílohy dodatku smlouvy v souladu s požadavky čl. 3 smlouvy.

4. Oprávnění užívat data, pravidla přístupu

4.1 Dodavatel odpovídá za dodržování pravidel přístupu definovaných v čl. 9.9 smlouvy, případně bezpečnostních pravidel distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.

4.2 Dodavatel zejména odpovídá za aktuálnost seznamu pracovníků oprávněných přistupovat do objektů a k informačním / komunikačním systémům objednatele. Při ukončení pracovně-právního vztahu nebo převedení na jinou funkci pracovníka oprávněného k přístupu je dodavatel o této skutečnosti povinen neprodleně informovat objednatele prostřednictvím kontaktních osob uvedených v Příloze 3 smlouvy a následně iniciovat aktualizaci příslušných seznamů oprávněných pracovníků. Seznam oprávněných pracovníků se zasílá e-mailem kontaktní osobě objednatele uvedené v čl. 14.3 smlouvy.

4.3 Veškerá komunikace dle tohoto článku bude probíhat elektronicky podepsanými e-mailovými zprávami. Akceptovatelné jsou například technologie elektronických podpisů odpovídající standardu OpenPGP.

5. Autorská a licenční práva

5.1 Závazky dodavatele jsou popsány v čl. 14.4 smlouvy.

6. Dodržování bezpečnostní politiky objednatele

6.1 Manažer kybernetické bezpečnosti objednatele bude informovat elektronicky podepsanými e-mailovými zprávami o všech relevantních změnách a dodatcích v bezpečnostních politikách Objednatele kontaktní osobu dodavatele uvedeného v čl. 17.6 této přílohy dodatku smlouvy.

6.2 Dodavatel zajistí zapracování akceptovaných bezpečnostních politik Objednatele, včetně publikovaných změn, do svých interních bezpečnostních politik, které předloží ke schválení Objednateli.

6.3 Dodavatel zajistí u všech svých pracovníků, kteří se podílejí na plnění povinností dle této přílohy dodatku resp. smlouvy, prokazatelné seznámení se svými bezpečnostními politikami.

7. Soulad s obecně závaznými právními předpisy

7.1 Dodavatel se zavazuje poskytovat servisní podporu dle smlouvy řádným způsobem a v souladu s platnými normami a obecně závaznými právními předpisy, které se na tento druh činnosti vztahují. Veškeré škody, které vzniknou porušením těchto norem a předpisů ze strany dodavatele, jdou k tíži dodavatele.

8. Řízení změn

8.1 Dodavatel je povinen řídit rizika související s plněním dle smlouvy, včetně zbytkových rizik. Na vyžádání manažera kybernetické bezpečnosti objednatele nebo osob provádějících kontrolní činnost dle čl. 15 této přílohy dodatku smlouvy je povinen způsob řízení těchto rizik doložit.

8.2 Dodavatel bere na vědomí, že objednatel při provádění změn postupuje v souladu s § 11 vyhlášky o kybernetické bezpečnosti.

8.3 U významných změn provádí objednatel analýzu rizik v souladu s metodikou CRAMM, nástrojem RAMSES.

8.4 Dodavatel a všichni subdodavatelé poskytnou objednateli nezbytnou součinnost a budou nápomocni při řízení změn, zejména při pravidelném hodnocení rizik a kontrole zavedených bezpečnostních opatření prováděných osobami určenými objednatelem.

8.5 [redacted]

9. Informační povinnost

9.1 Dodavatel bezodkladně informuje objednatele prostřednictvím kontaktních údajů uvedených v čl. 17.3 této přílohy dodatku smlouvy, pokud zjistí narušení bezpečnosti informací v důsledku kybernetické bezpečnostní události a poskytne objednateli dostatečné informace, které umožní splnění všech povinností odstranit následky takové události, vyšetřit ji a ohlásit ji Národnímu úřadu pro kybernetickou bezpečnost v souladu

s požadavky vyhlášky o kybernetické bezpečnosti. Dodavatel je povinen při těchto úkonech spolupracovat a přijmout finančně přiměřené kroky, které si objednatel vyžádá.

9.2 Dodavatel prostřednictvím kontaktních údajů uvedených v čl. 17.4 průběžně a bezodkladně informuje objednatele o všech jemu známých hrozbách a zranitelnostech, které by mohly mít vliv na hodnocení rizik prováděných objednatelem.

9.3 Dodavatel prostřednictvím manažera kybernetické bezpečnosti objednatele bezodkladně informuje objednatele o významné změně ovládání dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy s objednatelem.

9.4 Podrobnější podmínky ohlašování a klasifikace událostí jsou uvedeny v bezpečnostních pravidlech distribuovaných v souladu s čl. 6 této přílohy dodatku smlouvy.

10. Řízení kontinuity

10.1 Dodavatel postupuje při zajišťování kontinuity v souladu s pokyny předávanými oprávněnými osobami, jejichž kontaktní údaje jsou uvedeny v Příloze 3 smlouvy.

11. Podmínky předávání dat

11.1 Veškeré provozní údaje, databáze, soubory, obsah logů, ostatní data a informace poskytnuté a zpracovávané v souvislosti s předmětem plnění smlouvy jsou ve výhradním vlastnictví objednatele.

11.2 Předávání dat musí probíhat tak, aby nemohly neoprávněné osoby údaje číst, kopírovat, měnit ani mazat.

11.3 Uchovávání předávaných dat na datových nosičích (mobilní, ftp server) musí být zabezpečené proti přístupu neoprávněných osob.

12. Subdodavatelé

12.1 Dodavatel může i nadále využívat služeb subdodavatelů, kteří ke dni podpisu dodatku provádějí činnosti nebo jimž jsou zpřístupňována data ve smyslu tohoto dodatku, pokud splní povinnosti stanovené příslušnými právními předpisy, zejména vyhláškou o kybernetické bezpečnosti. Dodavatel předloží objednateli ke dni podpisu dodatku ke smlouvě seznam již využívaných subdodavatelů.

12.2 Dodavatel objednatele předem písemně informuje o úmyslu určit nového subdodavatele, včetně detailů činností, které má subdodavatel provádět a zpřístupňovaných dat. Pokud do 30 dnů od obdržení tohoto oznámení objednatel sdělí dodavateli písemně jakékoliv námitky (z přiměřených důvodů) k navrhovanému určení, dodavatel nesmí navrhovanému subdodavateli přidělit žádné činnosti ani zpřístupnit žádná data vážící se k plnění dle tohoto dodatku, s výjimkou předchozího písemného souhlasu poskytnutého objednatelem.

12.3 Pokud dodavatel sjedná se subdodavatelem provádění činností nebo zpřístupňování dat ve smyslu tohoto dodatku, je povinen uzavřít se subdodavatelem smlouvu nebo jiný právní akt, jež zakládá stejná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti jako jsou stanovené v tomto dodatku. Jedná se zejména o poskytnutí dostatečných záruk pro provedení vhodných technických a organizačních opatření tak, aby zpracování odpovídalo požadavkům vyhlášky o kybernetické bezpečnosti.

12.4 Ve vztahu ke každému subdodavateli, dodavatel:

a) vynaloží veškeré přiměřené úsilí, aby prověřil, že subdodavatel poskytuje úroveň ochrany v oblasti informační a kybernetické bezpečnosti, jež je vyžadována smlouvou;

b) zajistí, aby při řetězení subdodavatelů byla vzájemná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti upravena písemnou smlouvou obsahující podmínky, které nabízejí alespoň stejnou úroveň ochrany jako ty, které jsou uvedeny v tomto dodatku resp. ve smlouvě, a splňují požadavky vyhlášky o kybernetické bezpečnosti;

c) Dodavatel se zavazuje předložit Objednateli, na základě jeho písemného vyzvání, příslušnou smlouvu se subdodavatelem, s výjimkou informací, které jsou chráněné jako obchodní tajemství; osobní údaje; informace, které jsou chráněny smlouvou o zachování mlčenlivosti a utajovaných informací dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů;

d) zajistí, aby každý subdodavatel plnil povinnosti vyplývající z tohoto dodatku, které se vztahují na ochranu v oblasti informační a kybernetické bezpečnosti prováděnou tímto subdodavatelem, jako by byl stranou této smlouvy namísto dodavatele.

13. Bezpečnostní podmínky při ukončení smlouvy

13.1 Dodavatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech distribuovaných podle čl. 6 této přílohy dodatku smlouvy.

14. Pravidla pro likvidaci dat

14.1 Dodavatel při ukončení smlouvy zajistí splnění podmínek stanovených v bezpečnostních pravidlech distribuovaných podle čl. 6 této přílohy dodatku smlouvy.

15. Kontrola

15.1 Dodavatel a všichni subdodavatelé zpřístupní na vyžádání všechny informace nezbytné pro prokázání souladu s tímto dodatkem a umožní a budou nápomocni při auditech a inspekcích, jakýmkoli auditorem pověřeným objednatelem.

15.2 S přiměřeným předstihem před zahájením kontroly informuje objednatel dodavatele o této kontrole. Objednatel dále vynaloží přiměřené úsilí, aby prováděním kontroly nedošlo ke vzniku škody, nadměrného narušení prostor, zařízení, personálu a činnosti dodavatele. Dodavatel není povinen při provádění umožnit přístup do svých prostor pouze v případě, že:

a) osoba provádějící kontrolu nepředloží doklad totožnosti a pověření k provedení kontroly;

b) je kontrola prováděna mimo běžnou pracovní dobu, leda že kontrola pro splnění svého účelu vyžaduje provedení právě mimo běžnou pracovní dobu a kontrolující předem (v běžnou pracovní dobu) oznámil dodavateli, že se jedná o takový případ.

15.3 Dodavatel bere na vědomí, že objednatel provádí periodické hodnocení dodavatelů v souladu s požadavky normy ČSN ISO/IEC 9001.

16. Ustanovení o sankcích za porušení povinností

16.1 Pokud dodavatel způsobí škodu porušením povinností uvedených v tomto dodatku, případně porušením povinností uvedených v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy smlouvy, jak byly zapracovány do interních bezpečnostních politik

dodavatele, je povinen ji na vyžádání objednatele bezodkladně nahradit (nejpozději však do 10 dnů ode dne, kdy byla výše škody dodavateli objednatelem oznámena).

16.2 Je-li újma způsobena subdodavatelem, je povinen k náhradě újmy společně s dodavatelem, a to společně a nerozdílně.

16.3 Pokud dodavatel poruší podmínky režimu vstupu a vjezdu vozidel do objektů a na pozemky objednatele uvedené v čl. 9.5 smlouvy a/nebo povinnosti uvedené v čl. 4 této přílohy dodatku smlouvy a dále upřesňované v bezpečnostních pravidlech schválených dle čl. 6 této přílohy dodatku smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 10.000,- Kč (slovy: desettisíc korun českých) za každý jednotlivý případ porušení.

16.4 Pokud dodavatel poruší podmínky zabezpečení koncové pracovní stanice stanovené v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, jak byly zapracovány do interních bezpečnostních politik dodavatele, je objednatel oprávněn požadovat smluvní pokutu ve výši 20.000,- Kč (slovy: dvacettisíc korun českých) za každý jednotlivý případ porušení.

16.5 Pokud dodavatel poruší ohlašovací povinnost v oblasti bezpečnostních událostí / incidentů stanovenou v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy Smlouvy, jak byly zapracovány do interních bezpečnostních politik dodavatele, je objednatel oprávněn požadovat smluvní pokutu ve výši 100.000,- Kč (slovy: jednostotisíc korun českých) za každý jednotlivý případ porušení.

16.6 Pokud dodavatel nezajistí v určeném termínu realizaci nápravných opatření vyplývajících ze zákaznického auditu provedeného dle podmínek popsaných v čl. 15 této přílohy dodatku smlouvy a dále upřesňované v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, jak byly zapracovány do interních bezpečnostních politik dodavatele, je objednatel oprávněn požadovat smluvní pokutu ve výši 50.000,- Kč (slovy: padesáttisíc korun českých) za každý jednotlivý případ porušení.

16.7 Pokud dodavatel poruší ostatní povinnosti uvedené v této příloze dodatku smlouvy, případně v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy dodatku smlouvy, jak byly zapracovány do interních bezpečnostních politik dodavatele, je objednatel oprávněn požadovat smluvní pokutu ve výši 20.000,- Kč (slovy: dvacettisíc korun českých) za každý jednotlivý případ porušení.

16.8 Zaplacením smluvní pokuty nezaniká objednateli nárok na náhradu újmy v plné výši.

16.9 Porušení povinností stanovených dodavateli v tomto dodatku, případně v bezpečnostních pravidlech zasílaných dle čl. 6 této přílohy smlouvy, jak byly zapracovány do interních bezpečnostních politik dodavatele, a/nebo významná změna kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy může být důvodem k jednostrannému ukončení smlouvy ze strany objednatele.

17. Kontaktní údaje osob odpovědných za informační a/nebo kybernetickou bezpečnost

17.1 Kontaktní údaje osoby odpovědné za informační bezpečnost (manažera kybernetické bezpečnosti) na straně objednatele:

[redacted]

17.2 Kontaktní údaje osob odpovědných za vedení seznamu osob oprávněných k přístupu dle čl. 4.2 této přílohy dodatku smlouvy na straně objednatele:

Osoby uvedené v čl. 14.3 smlouvy

17.3 Kontakt pro zvládání bezpečnostních událostí, incidentů a zajištění kontinuity činností na straně objednatele:

Supervisor příslušného technického sálu – kontakty uvedeny v Příloze 3 smlouvy

17.4 Kontaktní údaje CSRT týmu objednatele:

[redacted]

17.5 Kontaktní údaje osoby odpovědné za režim vstupu a vjezdu do areálů, objektů a na pozemky objednatele.

[redacted]

17.6 Kontaktní údaje manažera kybernetické bezpečnosti / osoby odpovědné za informační bezpečnost na straně dodavatele:

[redacted]

17.7 Kontakt pro zvládání bezpečnostních událostí, incidentů a zajištění kontinuity činností na straně dodavatele:

[redacted]