

SMLOUVA NA UPGRADE INTERNÍHO FIREWALLU PRO ZAJIŠTĚNÍ BEZPEČNOSTNÍ SEGMENTACE A DOHLEDU INTERNÍ SÍTĚ LAN

Smluvní strany:

Hlavní město Praha

se sídlem: Mariánské nám. 2/2, Praha 1, PSČ: 110 01

IČO: 00064581, DIČ: CZ00064581

bankovní spojení: PPF banka, a.s., č. účtu: 27-0005157998/6000

zastoupené: Mgr. Jiřím Károlým, ředitelem odboru informatických činností
Magistrátu hl. m. Prahy

Číslo smlouvy Objednatele: INO/40/05/003714/2022

(dále jen „**Objednatel**“)

a

Corpus Solutions a.s.

se sídlem: Štětkova 1638/18, 140 00 Praha 4

IČO: 25764616, DIČ: CZ25764616

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze
oddíl B, vložka 5936

bank. spojení: Raiffeisenbank a.s., č. účtu: 69474001/5500

zastoupená: Ing. Tomášem Příbylem, předsedou představenstva

Číslo smlouvy Dodavatele: 2022-003-TP

(dále jen „**Dodavatel**“)

(Objednatel a Dodavatel dále společně jen „**Smluvní strany**“ anebo samostatně „**Smluvní strana**“)

dnešního dne uzavřely tuto smlouvu v souladu s ustanovením § 1746 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**OZ**“) a na základě zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“); (dále jen „**Smlouva**“)

Smluvní strany, vědomy si svých závazků obsažených v této Smlouvě a s úmyslem být touto Smlouvou vázány, se dohodly na následujícím znění Smlouvy:

1. ÚVODNÍ USTANOVENÍ

1.1. Objednatel prohlašuje, že:

1.1.1.je veřejnoprávní korporací; a

1.1.2.splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2. Dodavatel prohlašuje, že:

1.2.1.je podnikatelem dle ustanovení § 420 a násl. OZ;

1.2.2.splňuje veškeré podmínky a požadavky ve Smlouvě stanovené a je oprávněn Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

1.2.3.je osobou držící potvrzení, certifikaci či podobné rozhodnutí výrobce dodávaných zařízení či jeho oficiálního zastoupení o tom, že je oprávněn dodávat plnění, které je předmětem této Smlouvy, pokud výrobce dodávaných zařízení vyžaduje pro činnosti dle Smlouvy takové potvrzení, certifikace či podobné rozhodnutí;

1.2.4.ke dni uzavření Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení, ve znění pozdějších předpisů, a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat;

1.2.5.se náležitě seznámil se všemi podklady, které byly součástí zadávací dokumentace Veřejné zakázky včetně všech jejích příloh a které stanovují požadavky na plnění dle Veřejné zakázky. Zadávací dokumentace je ke dni uzavření Smlouvy dostupná na profilu Objednatele jako zadavatele;

1.2.6.je odborně způsobilý ke splnění všech svých závazků podle Smlouvy;

1.2.7.se detailně seznámil s rozsahem a povahou plnění dle Veřejné zakázky, a to tak, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci této Smlouvy a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci této Smlouvy za dohodnuté smluvní ceny uvedené ve Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění Veřejné zakázky;

1.2.8.jím poskytované plnění dle této Smlouvy odpovídá všem požadavkům vyplývajícím z platných právních předpisů, které se na plnění vztahují.

- 1.3. Pojmy s velkými počátečními písmeny definované ve Smlouvě budou mít význam, jenž je jim ve Smlouvě, včetně jejích příloh a dodatků, připisován.
- 1.4. Objednatel dne 5.8.2022 odesláním Oznámení o zahájení zadávacího řízení do Věstníku veřejných zakázek zahájil zadávací řízení na veřejnou zakázku s názvem „*Upgrade interního firewallu pro zajištění bezpečnostní segmentace a dohledu interní sítě LAN*“ (dále jen „**Veřejná zakázka**“), zadávané v rámci otevřeného řízení dle ZZVZ (dále také „**Zadávací dokumentace**“). Na základě zadávacího řízení byl Dodavatel vyzván k uzavření této Smlouvy na plnění předmětu Veřejné zakázky.

2. ÚČEL SMLOUVY

- 2.1. Objednatel je provozovatelem klíčových informačních systémů a dalších ICT služeb jak pro vlastní úřad Magistrátu hlavního města Prahy, tak pro jednotlivé městské části a řízené a podřízené organizace. Jedním z klíčových prvků, který je součástí bezpečnostního řešení, je systém interních firewallů pro zajištění bezpečnostní segmentace a dohledu interních LAN sítí. Na základě revize architektury bezpečnostních technologií a síťového prostředí, a porovnání možných variant řešení byl navržen funkční upgrade stávající technologie.
- 2.2. Účelem této Smlouvy je realizace Veřejné zakázky dle zadávacích podmínek Veřejné zakázky, tedy zejména obnovy stávajícího interního firewallu Objednatele, a to zajištěním podmínek pro dodávku, podporu a údržbu technologie Objednatele a zajištění dalších souvisejících služeb, to vše v souladu s požadavky Objednatele definovanými touto Smlouvou a zadávacími podmínkami Veřejné zakázky.
- 2.3. Dodavatel touto Smlouvou garantuje Objednateli splnění zadání Veřejné zakázky a všech z toho vyplývajících podmínek a povinností podle Zadávací dokumentace. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že:
- 2.3.1. v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy, budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel Veřejné zakázky vyjádřený Zadávací dokumentací;
 - 2.3.2. v případě chybějících ustanovení této Smlouvy budou použita dostatečně konkrétní ustanovení Zadávací dokumentace;
 - 2.3.3. Dodavatel je vázán svou nabídkou předloženou Objednateli v rámci zadávacího řízení na zadání Veřejné zakázky, která se pro úpravu vzájemných vztahů vyplývajících z této Smlouvy použije subsidiárně.

3. PŘEDMĚT SMLOUVY

3.1. Předmětem této Smlouvy je poskytnutí plnění sestávajícího z komplexní dodávky technologie pro obnovu interního firewallu a poskytování souvisejících služeb dle odst.

3.2 této Smlouvy (dále jen „**Plnění**“).

3.2. Předmět Plnění Dodavatele se skládá především z:

3.2.1. provedení detailní analýzy požadavků Objednatele na dodávku technologických prvků dle této Smlouvy a IT prostředí Objednatele, a vytvoření návrhu postupu implementace hardware v rámci technického vybavení Objednatele (dále jen „**Implementační plán**“). Implementační plán bude obsahovat upřesnění technických parametrů hardware a jeho implementace, bude obsahovat rozpracování akceptačních kritérií a bude v souladu se specifikací funkčních a dalších požadavků na hardware dle Technické specifikace, jak je definována v **Příloze č. 1** této Smlouvy („dále jen „**Technická specifikace**““);

3.2.2. dodání hardware (HW), tedy fyzicky existující technická zařízení a vybavení odpovídající parametrům Objednatele uvedených v Technické specifikaci, a to tam samostatně uvedených jednotlivých zařízení (dále vše souhrnně jen „**hardware**“ nebo „**Dodávka hardware**“), vč. zajištění software nezbytného pro fungování hardware, přičemž detailní specifikace Dodávky hardware je blíže určena v Technické specifikaci;

3.2.3. zajištění implementace a konfigurace Dodávky hardware vč. software v prostředí Objednatele, vč. nezbytných kroků instalace a zajištění nezbytného programového vybavení pro provoz prvků v prostředí Objednatele, a to v souladu s Implementačním plánem a za dodržení podmínek dále stanovených ve Smlouvě (dále jen „**Implementace**““);

3.2.4. zajištění podpory výrobce na dobu třiceti šesti (36) měsíců ode dne akceptace poslední dílčí Dodávky hardware blíže specifikované v této Smlouvě (dále jen „**Podpora výrobce**““), a to pro veškerý hardware dodaný Dodavatelem Objednateli na základě této Smlouvy;

3.2.5. zajištění provozní podpory v rozsahu vymezeném v **Příloze č. 3** Smlouvy (dále jen „**Provozní podpora**““).

3.3. Objednatel se zavazuje zaplatit Dodavateli dohodnutou cenu za řádně a včas poskytnuté Plnění, to vše za podmínek dále stanovených touto Smlouvou.

3.4. Dodavatel se zavazuje alokovat na poskytování Plnění dle této Smlouvy kapacity členů realizačního týmu Dodavatele a poskytovat Plnění dle Smlouvy za účasti členů realizačního týmu uvedeného v **Příloze č. 6** této Smlouvy, jimiž Dodavatel prokázal svou

kvalifikaci v zadávacím řízení Veřejné zakázky. Alokací kapacity se rozumí dostupnost kteréhokoliv člena realizačního týmu nebo jeho odpovídajícího náhradníka, jenž má minimálně stejnou kvalifikaci jako nahrazovaný člen. Jakákoliv dodatečná změna členů realizačního týmu musí být předem projednána a písemně schválena Objednatelem, přičemž změna bude Objednatelem schválena v případě, že Dodavatel nahradí osobu realizačního týmu takovou osobou, která prokazatelně disponuje srovnatelnými znalostmi a odbornou kvalifikací.

- 3.5. Dodavatel se zavazuje poskytovat Plnění sám, nebo s využitím poddodavatelů uvedených v **Příloze č. 6** této Smlouvy. Jakákoliv dodatečná změna osoby poddodavatele nebo rozsahu Plnění svěřených poddodavateli musí být předem písemně schválena Objednatelem, ledaže by plnění původně svěřené poddodavateli realizoval Dodavatel sám. Smluvní strany výslovně uvádějí, že při poskytování Plnění prostřednictvím jakékoliv třetí osoby dle tohoto odstavce má Dodavatel odpovědnost, jako by poskytování Plnění realizoval sám.

4. DOBA A MÍSTO PLNĚNÍ

- 4.1. Dodavatel se zavazuje dodat/poskytovat Plnění v souladu s Harmonogramem, který tvoří **Přílohu č. 4** této Smlouvy (dále jen „**Harmonogram**“).
- 4.2. Místem plnění jsou zejména sídlo Objednatele, sídla městských částí Objednatele a organizací zřizovaných Objednatelem, nebo sídla Objednatelem určených třetích osob, datová centra Objednatele a dále též jiné prostory dle potřeby a výslovného pokynu Objednatele.
- 4.3. Pokud to povaha plnění této Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Dodavatel oprávněn poskytovat části Plnění také vzdáleným přístupem.

5. IMPLEMENTAČNÍ PLÁN, DODÁVKA HARDWARE A IMPLEMENTACE

Implementační plán

- 5.1. Dodavatel se zavazuje vypracovat Implementační plán, ve kterém zejména:
- 5.1.1. popíše technický postup Dodávky hardware a Implementace hardware v prostředí Objednatele;
 - 5.1.2. vymezí nezbytné kroky a požadovanou součinnost Objednatele při Dodávce hardware a Implementaci;
 - 5.1.3. specifikuje standardní software dle odst. 12.5 této Smlouvy, který bude tvořit součást Plnění dle této Smlouvy;
 - 5.1.4. navrhne a rozpracuje detailní harmonogram prací Implementace.
- 5.2. Dodavatel předá Objednateli Implementační plán k akceptaci dle čl. 8 této Smlouvy v termínech dle Harmonogramu. Dodavatel zapracuje připomínky Objednatele

bez zbytečného prodlení a předá Implementační plán k opětovnému schválení Objednateli. V případě, že Objednatel odmítne zcela akceptovat Implementační plán Dodavatele, sjednávají Smluvní strany oprávnění Objednatele na vyhrazenou změnu závazku, a to změnu dodavatele Veřejné zakázky v souladu s § 222 odst. 10 ZZVZ, přičemž Dodavatele nahradí dodavatel, jehož nabídka byla vyhodnocena jako druhá v pořadí. V případě postupu dle § 222 odst. 10 ZZVZ se přiměřeně uplatní zákaz odstoupení od Dodávky hardware dle odst. 19.5 Smlouvy.

Dodávka hardware

- 5.3. Dodavatel prohlašuje, že veškeré dodávané plnění je získáno legálně a umožňuje využití těchto hardware a software Objednatelem, jakožto koncovým zákazníkem, v souladu s distribučními a licenčními podmínkami výrobce zařízení.
- 5.4. Dodavatel doloží Objednateli (současně s Dodávkou hardware a nejpozději do pěti (5) pracovních dnů ode dne písemné žádosti Objednatele) potvrzení výrobce či jeho oficiálního zastoupení, že dodávané plnění (seznam sériových čísel) je určeno pro koncového zákazníka pro využití na území České republiky a že má Objednatel k tomuto plnění zajištění Podporu výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Objednatel, bude se jednat o porušení podmínky originálního a nového zařízení (viz níže odst. 5.7 této Smlouvy).
- 5.5. Dodavatel je povinen (na vyžádání Objednatele) současně s Dodávkou hardware doložit Objednateli položkový rozpad jednotlivých kusů hardware, které jsou předmětem Dodávky hardware, vč. rozpadu ceny za jednotlivé položky.
- 5.6. Dodavatel prohlašuje, že pro dodávané plnění platí, že Objednatel jako koncový zákazník není nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaných zařízení a z Podpory výrobce, kterou tento výrobce k dodávaným hardware a software produktům poskytuje.
- 5.7. Dodavatel se zavazuje dodat Objednateli takový hardware, který bude:
 - 5.7.1.nový, nepoužitý a nerepasovaný;
 - 5.7.2.plně funkční;
 - 5.7.3.použitelný Objednatelem v České republice. Zejména v této souvislosti Dodavatel zaručuje Objednateli, že hardware získal veškerá nezbytná osvědčení pro užití v České republice, a to jak z pohledu obecně závazných právních předpisů, tak podmínek výrobce pro poskytování navazujících služeb maintenance. Dodavatel předá kopie těchto osvědčení při předání dodávky;
 - 5.7.4.určený pro evropský trh;
 - 5.7.5.mít jakost a provedení stanovené v této Smlouvě;

- 5.7.6. bez materiálových, konstrukčních, výrobních a vzhledových či jiných vad;
 - 5.7.7. splňovat veškeré nároky a požadavky českého právního řádu, zejména zákona č. 541/2020 Sb., o odpadech, ve znění pozdějších předpisů (dále jen „**zákon o odpadech**“) a zákona č. 477/2001 Sb., o obalech, ve znění pozdějších předpisů;
 - 5.7.8. dodán včetně všech souvisejících systémových licencí specifikovaných v Implementačním plánu či jiných systémových licencí nezbytných k řádnému využívání hardware v rozsahu a za podmínek této Smlouvy vč. jejích příloh;
 - 5.7.9. bezpečný, zejména že dodávky neobsahují radioaktivní materiály a jiné nebezpečné látky a věci, které se mohou stát nebezpečným odpadem ve smyslu zákona o odpadech;
 - 5.7.10. ve vlastnictví Dodavatele a který je Dodavatel bez dalšího oprávněn na Objednatele převést; a
 - 5.7.11. není zatížen zástavními, předkupními, nájemními či jinými právy třetích osob.
- 5.8. Dodavatel zaručuje Objednateli, že dodaný software bude plně funkční a způsobilý pro použití k určenému účelu a pro užití v České republice, odpovídat sjednané specifikaci, bez faktických vad, a bude splňovat veškeré nároky a požadavky českého právního řádu.
- 5.9. Dodavatel prohlašuje, že software nemá žádné právní vady, zejména ohledně něj není veden žádný soudní spor, jsou uhrazeny všechny daně a poplatky týkající se software.

Implementace

- 5.10. Implementace bude poskytnuta v souladu s Harmonogramem a postupem dle Implementačního plánu.
- 5.11. Dodavatel se dále zavazuje vytvořit do třiceti (30) dnů od dokončení Implementace tzv. dokumentační základnu Implementace (dále jen „**Dokumentace**“), ve které budou obsaženy veškeré dokumenty vztahující se k provádění Implementace, infrastruktura hardware a Plnění této Smlouvy jako celku, a to zejména:
- 5.11.1. veškeré specifikace, manuály či licenční podmínky veškerého hardware, software a jiného plnění poskytnutého Objednateli po nabytí účinnosti této Smlouvy;
 - 5.11.2. veškeré technické podmínky a normy, dle kterých je Plnění prováděno či poskytováno;
 - 5.11.3. veškeré dokumenty, které Dodavatel obdržel od Objednatele a které se vztahují k infrastruktuře hardware nebo k poskytování Implementace;

příčemž se Dodavatel zavazuje při přípravě Dokumentace respektovat a zachovat závazné vzory poskytnuté ke dni účinnosti Smlouvy Objednatelem.

- 5.12. Dokumentace bude rozdělena dle jednotlivých kategorií dokumentů uvedených výše a bude Objednateli nepřetržitě přístupná on-line. Dokumentace podléhá akceptaci dle čl. 8 Smlouvy. Dodavatel je povinen pravidelně, nejméně 1x ročně, prověřit aktuálnost Dokumentace tak, aby obsahovala veškeré dokumenty spadající do výše uvedených kategorií vztahující se k Plnění dle této Smlouvy a infrastruktúře hardware. Každý dokument musí být do Dokumentace vložen Dodavatelem nejpozději do třiceti (30) dnů od poskytnutí Plnění, ke kterému se tento dokument vztahuje.

6. POSKYTOVÁNÍ PODPORY

Podpora výrobce

- 6.1. Dodavatel se zavazuje zajistit Podporu výrobce k hardware, a to po dobu třiceti šesti (36) měsíců od akceptace Dodávky hardware.
- 6.2. Dodavatel je s Dodávkou hardware dle Smlouvy a po dobu poskytování Podpory výrobce dle této Smlouvy povinen:

6.2.1.mít uzavřenou dohodu o podpoře s výrobcem hardware na všechen dodaný hardware tak, aby v případě závady na dodaném hardware, kterou není Dodavatel schopen sám odstranit v rámci Provozní podpory, bylo možné eskalovat závadu přímo k výrobcu hardware nebo jím pověřenému servisnímu partnerovi;

6.2.2.zajistit Objednateli přístup k dokumentaci výrobce hardware a znalostní bázi, kterou výrobce hardware v rámci své Podpory výrobce poskytuje;

6.2.3.zajistit přímý přístup k Podpoře výrobce, včetně možnosti si sám a přímo otevřít požadavek na Podporu výrobce, provádět změny priority požadavků a případné eskalace pracovníky Objednatele, a to po celou dobu, po kterou výrobce poskytuje na dané zařízení podporu.

- 6.3. Po dobu poskytování Podpory výrobce je Dodavatel dále povinen:

6.3.1.poskytnout Objednateli všechny relevantní software releases a verze software tak, aby dodané řešení vyhovovalo zadání Objednatele a fungovalo bez závad;

6.3.2.informovat Objednatele o nových verzích a funkcích hardware a souvisejícího software, které mohou rozšiřovat dodané řešení způsobem, který Objednatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení (software);

6.3.3.zajistit službu hlášení softwarových chyb, které jsou oznámeny výrobcem.

6.4. Specifikace Podpory výrobce je dále uvedena v **Příloze č. 2** této Smlouvy.

Provozní podpora

6.5. Dodavatel je povinen poskytovat Objednateli Provozní podporu v rozsahu dle katalogových listů, které tvoří **Přílohu č. 3** této Smlouvy a za podmínek a v parametrech specifikovaných dále v této Smlouvě.

7. SOUČINNOST SMLUVNÍCH STRAN

7.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.

7.2. Objednatel je povinen spolupracovat s Dodavatelem a poskytovat mu veškerou nutnou součinnost potřebnou pro řádné poskytování Plnění, vč. např. zajištění odpovídajícím způsobem vybaveného pracovního místa pracovníkům Dodavatele na pracovišti Objednatele. Objednatel je povinen informovat Dodavatele o veškerých skutečnostech, které jsou nebo mohou být důležité pro Plnění této Smlouvy.

7.3. Objednatel je povinen zajistit Dodavateli veškerou potřebnou součinnost zaměstnanců Objednatele nebo třetích stran zajišťujících pro Objednatele služby v oblasti ICT v rozsahu potřebném pro řádné plnění dle této Smlouvy. Nesplnění pokynů při plnění pouze v důsledku nezajištění výše uvedené součinnosti nebude považováno za porušení nebo nedodržení požadované kvality Plnění a nemůže být důvodem pro neakceptování Výkazu plnění dle odst. 9.5 Smlouvy Objednatelem.

7.4. V rámci součinnosti se Objednatel zavazuje umožnit Dodavateli užití vybraných hardware a software prostředků Objednatele, a to výhradně za účelem plnění předmětu této Smlouvy a pouze po dobu účinnosti této Smlouvy. Dodavatel se zavazuje užívat tyto prostředky řádně a v souladu s provozními a bezpečnostními postupy či pokyny Objednatele. Dodavatel se dále zavazuje, že nebude s těmito prostředky Objednatele nakládat nebo je používat v rozporu s touto Smlouvou.

7.5. Objednatel je povinen vyvinout úsilí k zajištění vzdáleného přístupu Dodavateli k serverům infrastruktury či k jiným částem IT prostředí Objednatele výhradně pro účely poskytování Plnění podle této Smlouvy.

7.6. Objednatel je povinen Dodavateli poskytnout veškeré podklady a informace nezbytné k poskytnutí Plnění.

7.7. Objednatel je povinen umožnit zaměstnancům Dodavatele, členům realizačního týmu anebo jiným osobám Dodavatele zajišťujícím poskytnutí Plnění vstup do míst plnění podle této Smlouvy. Jedná se zejména o zajištění přístupu do míst, kde jsou umístěny produkční servery. Za zajištění přístupu odpovídá Objednatel.

7.8. Pokud Objednatel neposkytne v odst. 7.1 této Smlouvy dohodnutou součinnost, má Dodavatel právo požadovat na Objednateli posunutí stanovených termínů o čas, po který Dodavatel nemohl pracovat na plnění Smlouvy.

8. AKCEPTACE

8.1. Každý výsledek Plnění dle této Smlouvy, který představuje samostatný předmět způsobilý přejímky (dále jen „**Dílčí plnění**“), bude Objednatelem akceptován na základě akceptační procedury. Akceptační procedura zahrnuje ověření, zda Dodavatelem poskytnuté Dílčí plnění je výsledkem, ke kterému se Dodavatel zavázal, a to porovnáním skutečných vlastností jednotlivých Dílčích plnění Dodavatele s jejich závaznou specifikací uvedenou v této Smlouvě nebo jiném dohodnutém závazném dokumentu za využití akceptačních kritérií tam stanovených nebo později pro tento účel dohodnutých Smluvními stranami.

8.2. Akceptace dokumentů

8.2.1. Dokumenty, které mají být podle této Smlouvy vypracované Dodavatelem a předané Objednateli, budou Objednatelem schválené a akceptované v souladu s akceptační procedurou definovanou v tomto odst. 8.2 Smlouvy.

8.2.2. Dodavatel se zavazuje průběžně konzultovat práce na zhotovení dokumentů s Objednatelem. Dodavatel je povinen předat dokumenty k akceptaci včas tak, aby mohly být dodrženy navazující termíny.

8.2.3. Objednatel je povinen vznést své výhrady nebo připomínky k dokumentu do deseti (10) pracovních dnů ode dne jejich doručení. Vznese-li Objednatel výhrady nebo připomínky k dokumentu, zavazuje se Dodavatel do pěti (5) pracovních dnů provést veškeré potřebné úpravy dokumentu dle výhrad a připomínek Objednatele a takto upravený dokument předat Objednateli k akceptaci. Pokud výhrady a připomínky Objednatele přetrvávají nebo Objednatel identifikuje výhrady a připomínky nové, je Objednatel oprávněn postupovat podle tohoto odst. 8.2.3 Smlouvy i opakovaně.

8.2.4. V případě, že Objednatel nemá k dokumentu připomínky ani výhrady, zavazuje se ve lhůtě deseti (10) pracovních dnů od předložení dokumentu k akceptaci tento dokument akceptovat a potvrdit o tom písemný akceptační protokol.

8.2.5. Bude-li trvání akceptační procedury ovlivněné vznesením výhrad nebo připomínek Objednatele k dokumentu a potřebou jejich vyřešení, bude případné prodlení ve vztahu k dohodnutým termínům

pro akceptaci dokumentu či nedodržení harmonogramu přičteno k tíži Dodavatele.

8.3. Akceptace jiných Dílčích plnění než dokumentů

- 8.3.1. Umožňuje-li to povaha Plnění a nestanoví-li tato Smlouva jinak, bude akceptace jednotlivých Dílčích plnění provedena v souladu s akceptační procedurou definovanou v tomto odst. 8.3 této Smlouvy.
- 8.3.2. Předání a převzetí Objednatelem objednaných a Dodavatelem řádně provedených Dílčích plnění bude probíhat postupně, akceptací jednotlivých Dílčích plnění, a to v termínech uvedených v této Smlouvě nebo stanovených v souladu s touto Smlouvou.
- 8.3.3. Akceptační procedura zahrnuje ověření řádného provedení jednotlivých Dílčích plnění porovnáním jejich skutečných vlastností s jejich specifikací stanovenou touto Smlouvou; specifikací se rozumí i akceptační kritéria, jsou-li stanovena. Akceptační procedura zahrnuje také ověření, že Dílčí plnění k danému dni plně odpovídá platné legislativě a že nevyžaduje provedení jeho údržby.
- 8.3.4. Akceptační procedura bude zahrnovat akceptační testy, které budou probíhat na základě specifikace akceptačních testů připravených Dodavatelem. Nedohodnou-li se Smluvní strany jinak, přípravu scénářů, příkladů a dat na akceptační test zajistí Dodavatel za přiměřené součinnosti Objednatele, a to s ohledem na účel akceptační procedury dle této Smlouvy. Objednatel má právo vyjadřovat se a požadovat zapracování svých odůvodněných připomínek ke specifikaci akceptačních testů a dalším parametrům testování.
- 8.3.5. Dodavatel písemně vyzve Objednatele k účasti na akceptační proceduře a tuto písemnou výzvu doručí Objednateli nejméně pět (5) pracovních dnů před zahájením akceptační procedury. Pokud se Objednatel nedostaví v termínu určeném pro provedení akceptačních testů, přestože byl Dodavatelem k účasti řádně vyzván, je Dodavatel oprávněn provést příslušné akceptační testy bez jeho přítomnosti. O průběhu akceptačních testů vyhotoví Dodavatel písemný záznam, v němž zejména uvede, zda testy prokázaly chyby. Objednateli budou poskytnuty originály veškerých dokumentů vypracovaných v souvislosti s provedením akceptačních testů.
- 8.3.6. Jestliže jednotlivé Dílčí plnění splní akceptační kritéria akceptačních testů, Dodavatel se zavazuje nejpozději v pracovní den následující po ukončení akceptačních testů umožnit Objednateli toto Dílčí plnění převzít

a Objednatel se zavazuje k jeho převzetí nejpozději do deseti (10) pracovních dnů. Smluvní strany se zavazují o tomto převzetí sepsat akceptační protokol.

8.3.7. Nestanoví-li specifikace akceptačních testů ve Smlouvě či dle požadavků Objednatele jinak, musí Dílčí plnění splňovat všechna stanovená akceptační kritéria. Objednatel je oprávněn (nikoli však povinen) Dílčí plnění převzít i v případech, kdy počet a/nebo druh vad nebrání využití výsledků Dílčího plnění, v takovém případě je akceptační protokol podepsán s výhradou vč. uvedení doby pro odstranění vad nebránících využití výsledků Dílčího plnění.

8.3.8. Pokud kterékoliv z jednotlivých Dílčích plnění nesplňuje stanovená akceptační kritéria nebo je splňuje s vadami, které jsou přípustné, sdělí Objednatel své připomínky písemně Dodavateli. Pokud Objednatel takové Dílčí plnění současně akceptuje, uvede své připomínky v akceptačním protokolu. Nesdělení připomínek nebo neoznámení některé vady při akceptaci nemá vliv na povinnost Dodavatele tuto vadu odstranit, pokud o ní ví, dodatečně ji zjistí či mu bude dodatečně oznámena.

8.3.9. Dodavatel je povinen vypořádat připomínky Objednatele bez zbytečného odkladu a neprodleně předložit příslušné Dílčí plnění k opakované akceptaci dle této Smlouvy, za přiměřeného použití ostatních ustanovení tohoto čl. 8 Smlouvy. Akceptační procedura, včetně procesu testování a případných následných oprav, se bude opakovat, dokud příslušné Dílčí plnění nesplní akceptační kritéria pro příslušný akceptační test. V případě, že se jedná o vypořádání připomínek k Dílčímu plnění, které již bylo akceptováno, namísto akceptačního protokolu Smluvní strany potvrdí písemně, že připomínky byly vypořádány.

8.3.10. Dohodnuté termíny pro akceptaci Dílčího plnění nejsou dotčeny trváním akceptační procedury ani jakýmkoli jejím prodloužením z důvodu vad bránících akceptaci.

8.4. Lhůty uvedené čl. 8 Smlouvy platí, pokud se Smluvní strany nedohodnou prokazatelně písemně jinak.

9. CENA A PLATEBNÍ PODMÍNKY

9.1. Cena za Dodávku hardware a Podporu výrobce

9.1.1.Smluvní strany sjednávají cenu Dodávky hardware a Podpory výrobce ve výši uvedené v **Příloze č. 5** této Smlouvy, a to jako cenu za hardware, který je předmětem Dodávky hardware a cenu za Podporu výrobce k příslušnému hardware.

9.1.2.Smluvní strany prohlašují, že celková cena za Dodávku hardware a Podporu výrobce dle Smlouvy, uvedená v **Příloze č. 5** této Smlouvy, bude uhrazena až po poslední dílčí akceptaci Dodávky hardware a Podpory výrobce, tedy nikoli v dílčích splátkách.

9.2. Cena za Implementační plán a Implementaci

9.2.1.Cena za vyhotovení Implementačního plánu a provedení Implementace se odvíjí od jednotkové ceny za jeden (1) člověkodenní (dále jen „ČD“) a pevného maximálního počtu čtyřicet (40) ČD. Smluvní strany se dohodly, že pokud bude v modelu ceny vyhotovení Implementačního plánu a provedení Implementace překročen pevný počet ČD dle předchozí věty, nemá Dodavatel nárok na cenu „víceprací“. Smluvní strany se dále dohodly, že Objednatel je povinen hradit jen skutečně odpracovaný čas dle Výkazu plnění dle odst. 9.5 Smlouvy, který může být i nižší než maximální a nepřekročitelný počet čtyřicet (40) ČD.

9.2.2.Smluvní strany prohlašují, že celková cena za vyhotovení Implementačního plánu a provedení Implementace uvedená v **Příloze č. 5** této Smlouvy, bude uhrazena až po akceptaci postupem dle čl. 8 Smlouvy.

9.2.3.Cena za Implementaci a Implementační plán bude určena s přesností na celé člověkohodiny.

9.3. Cena za Provozní podporu

9.3.1.Smluvní strany sjednávají cenu Provozní podpory ve výši uvedené v **Příloze č. 3** této Smlouvy, a to jako měsíční sazbu, která Dodavateli přísluší za měsíc poskytování Provozní podpory.

9.3.2.Při nedodržení některého z parametrů Provozní podpory uvedeného v SLA dle **Přílohy č. 3** této Smlouvy (dále také jen „SLA“) má Objednatel nárok požadovat dohodnutou slevu, a to ve výši stanovené v tomto odst. 9.3.2 Smlouvy z měsíční ceny Provozní podpory dle této Smlouvy. Dohodnutá sleva se sjednává maximálně do výše 100 % ceny za poskytování Provozní podpory po celou dobu vyhodnocovacího období.

9.3.3. Níže uvedená tabulka zobrazuje výčet parametrů SLA s příslušnými slevami z příslušné ceny za poskytování Provozní podpory dle této Smlouvy a způsobem výpočtu:

Název parametru	Slevy z ceny příslušné měsíční ceny služby Provozní podpory v Kč (bez DPH)	Způsob výpočtu
Dostupnost Služby (jak je definována v Příloze č. 2 této Smlouvy)	1.000,-	Za každou započatou 1 hodinu nedostupnosti Služby nad stanovenou hodnotu parametru
Max. doba výpadku	750,-	Za každou započatou 1 hodinu nad stanovenou hodnotu parametru
Max. doba nedostupnosti dat	750,-	Za každou započatou 1 hodinu nad stanovenou hodnotu parametru
Max. doba servisní odezvy	500,-	Za každých započatých 30 minut nad stanovenou hodnotu parametru
Doba odstranění závady kategorie A	750,-	Za každou započatou 1 hodinu nad stanovenou hodnotu parametru
Doba odstranění závady kategorie B	500,-	Za každý započatý den nad stanovenou hodnotu parametru
Doba odstranění závady kategorie C	500,-	Za každý započatý den nad stanovenou hodnotu parametru

9.3.4. Dodavatel se zavazuje vypracovat za každé vyhodnocovací období zprávu o poskytování Provozní podpory, ze které bude zřejmé dodržování parametrů dle SLA (dále také „Zpráva“). Zpráva tvoří přílohu příslušné Faktury, jak je tato definována v odst. 9.10 této Smlouvy.

9.3.5. Cena Provozní podpory se může přiměřeně snížit o dohodnutou slevu určenou dle SLA, pokud dle příslušné Zprávy bude zřejmé, že Provozní podpora nebyla poskytována v závazných parametrech specifikovaných v SLA.

Společná cenová ujednání

- 9.4. V rámci realizace Dodávky hardware a Podpory výrobce Dodavatel předloží Objednateli spolu s Fakturou dodací list obsahující položkový rozpis ceny tohoto Plnění (dále jen „**Dodací list**“).
- 9.5. V rámci Implementace, Implementačního plánu a Provozní podpory Dodavatel předloží Objednateli spolu s Fakturou seznam realizovaných prací, který bude obsahovat rozpis plnění (dále jen „**Výkaz plnění**“), a to do deseti (10) dnů po konci příslušného měsíce.
- 9.6. Objednatel je povinen v době splatnosti dané Faktury přiložený Výkaz plnění a Zprávu schválit nebo uvést, ve které části neodpovídá skutečnosti.
- 9.7. Jednotkové ceny za poskytování Plnění dle **Přílohy č. 3** této Smlouvy jsou pevné a úplné, tj. zahrnují veškerá plnění dle Smlouvy v rámci poskytování jednotlivých Plnění. Ceny jsou uvedeny jako maximální, nejvýše přípustné, nepřekročitelné a zahrnující veškeré náklady, odměny či poplatky Dodavatele nezbytné k řádnému a včasnému poskytování Plnění.
- 9.8. Součástí ceny Plnění dle této Smlouvy je i cena za služby a dodávky, které v Zadávací dokumentaci nebo ve Smlouvě nejsou výslovně uvedeny, ale Dodavatel jakožto odborník o nich ví nebo má vědět, že jsou nezbytné pro řádné a včasné poskytování Plnění. Dodavatel nese veškeré náklady nutně nebo účelně vynaložené při plnění závazků ze Smlouvy včetně správních poplatků.
- 9.9. K Ceně za poskytnutí Plnění bude Dodavatelem připočteno DPH ve výši ke dni uskutečnění zdanitelného plnění.

Platební podmínky

- 9.10. Cena Plnění bude Objednatelem Dodavateli hrazena na základě daňového dokladu – faktury (dále jen „**Faktura**“). Dodavatel předloží Objednateli fakturu až po řádné akceptaci příslušného Dílčího plnění. Objednatelem potvrzený Dodací list, Akceptační protokol, Výkaz plnění či Zpráva budou vždy tvořit nedílnou přílohou příslušné Faktury.
- 9.11. Splatnost jednotlivých daňových dokladů – Faktur se sjednává na třicet (30) dnů ode dne jejich doručení povinné Smluvní straně. Toto ustanovení se uplatní i v případě hrazení smluvních pokut. Cena bude považována za uhrazenou dnem odeslání příslušné částky z účtu Objednatele na účet Dodavatele.
- 9.12. Všechny Faktury musí splňovat náležitosti řádného daňového dokladu požadované § 435 OZ a zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a vždy musí výslovně obsahovat následující údaje: označení Smluvních stran a jejich adresy, IČO, DIČ (je-li přiděleno), údaj o tom, že vystavovatel Faktury je zapsán v obchodním rejstříku včetně spisové značky, označení této Smlouvy, označení poskytnutých Plnění, jejich rozsah, jednotkovou a celkovou cenu, číslo faktury, den

vystavení a lhůtu splatnosti Faktury, označení peněžního ústavu a číslo účtu, na který se má platit, fakturovanou částku, razítko a podpis oprávněné osoby. Faktura bude vždy obsahovat příslušné Dodací listy, Akceptační protokoly vztahující se k jednotlivým částem Plnění a jiné přílohy požadované Objednatelem. Faktury budou znít na částku v českých korunách (Kč).

- 9.13. Nebude-li Faktura obsahovat stanovené náležitosti a přílohy, nebo v ní nebudou správně uvedené údaje dle této Smlouvy, je Objednatel oprávněn vrátit ji ve lhůtě její splatnosti Dodavateli. V takovém případě se přeruší běh lhůty splatnosti a nová lhůta splatnosti započne běžet doručením opravené Faktury.
- 9.14. Platby peněžitých částek se provádí bankovním převodem na účet druhé Smluvní strany, uvedený ve Faktuře. Peněžitá částka se považuje za zaplacenou okamžikem jejího odesání z účtu odesílatele ve prospěch účtu příjemce.
- 9.15. Objednatel neposkytuje Dodavateli na Plnění dle této Smlouvy jakékoliv zálohy.
- 9.16. V případě prodlení kterékoliv Smluvní strany se zaplacením peněžitě částky vzniká oprávněné Smluvní straně nárok na úrok z prodlení v zákonné výši dlužné částky za každý započatý den prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé újmy.
- 9.17. Objednatel bude hradit přijaté Faktury pouze na bankovní účty Dodavatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona č. 235/2004 Sb., o DPH, ve znění pozdějších předpisů (dále jen „**zákon o DPH**“). V případě, že Dodavatel nebude mít svůj bankovní účet tímto způsobem zveřejněn, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH uhradí Dodavateli až po zveřejnění příslušného účtu Dodavatele v registru plátců a identifikovaných osob Dodavatelem.
- 9.18. Dodavatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Dodavatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH (dále jen „**nespolehlivý plátc**“). V případě, že správce daně rozhodne o tom, že Dodavatel je nespolehlivým plátcem, zavazuje se Dodavatel o tomto informovat Objednatele do dvou (2) pracovních dní. Stane-li se Dodavatel nespolehlivým plátcem, uhradí Objednatel Dodavateli pouze základ daně, přičemž DPH bude Objednatelem uhrazena Dodavateli až po písemném doložení Dodavatele o jeho úhradě této DPH příslušnému správci daně.

10. PRÁVA A POVINNOSTI DODAVATELE

- 10.1. Dodavatel je povinen spolupracovat s Objednatelem a poskytovat mu veškerou součinnost potřebnou pro řádné poskytování/provádění Plnění podle této Smlouvy. Dodavatel je povinen písemně informovat Objednatele o veškerých skutečnostech, které jsou nebo mohou být důležité pro plnění Smlouvy.

10.2. Dodavatel je povinen poskytovat/provádět Plnění vlastním jménem, na vlastní odpovědnost a v souladu s pokyny Objednatele řádně a včas a s péčí řádného hospodáře odpovídající podmínkám sjednaným v této Smlouvě a s procesy „best practice“. Při plnění této Smlouvy je Dodavatel povinen upozorňovat Objednatele na nevhodnost jeho pokynů, které by mohly mít za následek újmu na právech Objednatele nebo vznik škody. Pokud Objednatel i přes upozornění na splnění svých pokynů trvá, neodpovídá Dodavatel za případnou škodu tím vzniklou.

10.3. Dodavatel se dále zavazuje:

10.3.1. zabalit zboží či jinak opatřit zboží pro přepravu způsobem zabraňujícím poškození zboží nebo znehodnocení;

10.3.2. dostane-li se Dodavatel do prodlení se svým plněním bez toho, aby to způsobil Objednatel či nastaly překážky vylučující povinnost k náhradě újmy po dobu delší než třicet (30) dnů, je Objednatel oprávněn zajistit náhradní plnění po dobu prodlení Dodavatele jinou osobou; v takovém případě se Dodavatel zavazuje nahradit v plném rozsahu náklady spojené s náhradním plněním;

10.3.3. poskytovat Plnění spočívající v instalaci, implementaci a veškeré konzultační, servisní či obdobné činnosti vztahující se k Plnění certifikovaným pracovníkem, který je oprávněn k provádění servisních zásahů na území České republiky;

10.3.4. upozorňovat Objednatele na všechny hrozící vady svého Plnění či potenciální výpadky Plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro plnění předmětu Smlouvy nezbytné;

10.3.5. neprodleně oznámit Objednateli jakékoli překážky, které mu brání v plnění předmětu Smlouvy a výkonu dalších činností souvisejících s plněním předmětu Smlouvy;

10.3.6. upozornit Objednatele na potenciální rizika vzniku škod a provést včas a řádně na své náklady taková opatření, která riziko sníží nebo zcela vyloučí;

10.3.7. upozorňovat Objednatele v odůvodněných případech na případnou nevhodnost pokynů Objednatele;

10.3.8. výslovně upozornit Objednatele, pokud by požadované Plnění vedlo ke zhoršení výkonu systémů Objednatele či vzniku poruch a škod, přičemž Dodavatel odpovídá za vzniklé škody Objednateli v plném rozsahu, pokud řádně Objednatele neinformoval;

- 10.3.9. i bez pokynů Objednatele provést nutné úkony, které, ač nejsou předmětem této Smlouvy, budou s ohledem na nepředvídatelné okolnosti pro plnění Smlouvy nezbytné nebo jsou nezbytné pro zamezení vzniku škody;
- 10.3.10. informovat Objednatele o plnění svých povinností podle této Smlouvy a o důležitých skutečnostech, které mohou mít vliv na výkon práv a plnění povinností Smluvních stran;
- 10.3.11. zajistit, aby všechny osoby podílející se na plnění Dodavatelových závazků z této Smlouvy, které se budou zdržovat v prostorách nebo na pracovištích Objednatele, dodržovaly účinné právní předpisy o bezpečnosti a ochraně zdraví při práci, jiné bezpečnostní, hygienické, požární, organizační a environmentální předpisy, předpisy o vstupu do objektů a veškeré interní předpisy Objednatele, s nimiž Objednatel Dodavatele předem obeznámil nebo které jsou všeobecně známé;
- 10.3.12. řešit písemné požadavky či dotazy Objednatele vztahující se k předmětu plnění dle této Smlouvy, a to nejpozději ve lhůtě pěti (5) pracovních dnů ode dne jejich doručení Dodavateli;
- 10.3.13. dodržovat ICT standardy, včetně všech jejich aktualizací, které mu budou Objednatelem předloženy pro účely realizace Plnění a současně další dokumenty, které budou tyto ICT standardy doplňovat nebo nahrazovat, přičemž **Přílohu č. 7** této Smlouvy tvoří seznam ICT standardů Objednatele, které byly Dodavateli předány při podpisu této Smlouvy; Objednatel se zavazuje Dodavateli předat veškeré aktualizace a nové ICT standardy, jejichž přijetí Dodavatel protokolárně potvrdí při předání.
- 10.4. Dodavatel je povinen při uzavření Smlouvy doplnit **Přílohu č. 2** této Smlouvy obchodními podmínkami výrobce hardware, přičemž tyto obchodní podmínky uvedené v **Příloze č. 2** této Smlouvy se použijí na další práva a povinnosti dle této Smlouvy podpůrně. V případě, že bude některé ustanovení **Přílohy č. 2** této Smlouvy v rozporu se zněním Smlouvy nebo jejích dalších příloh, mají přednost ustanovení Smlouvy a jejích dalších příloh.
- 10.5. Dodavatel se dále zavazuje udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou Dodavatelem třetí osobě (zejména Objednateli), a to tak, že limit pojistného plnění vyplývající z pojistné smlouvy, nesmí být nižší než 50.000.000,- Kč za rok, a to se spoluúčastí max. deset (10) %. Pojistnou smlouvu dle tohoto odstavce, pojistku potvrzující

uzavření takové smlouvy nebo pojistný certifikát potvrzující uzavření takové smlouvy je Dodavatel povinen předložit Objednateli nejpozději do sedmi (7) pracovních dnů po uzavření této Smlouvy a dále kdykoliv po písemném vyžádání Objednatele, a to do pěti (5) pracovních dnů od doručení písemného vyžádání. Nepředložením pojistné smlouvy, pojistky nebo pojistného certifikátu ve výše uvedených lhůtách vzniká právo Objednatele na odstoupení od Smlouvy.

Odpovědné zadávání

- 10.6. Dodavatel se zavazuje po celou dobu trvání smluvního vztahu založeného Smlouvou zajistit dodržování veškerých právních předpisů, zejména pak pracovněprávních (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění Smlouvy podílejí (a bez ohledu na to, zda budou činnosti prováděny Dodavatelem či jeho poddodavateli). Dodavatel se také zavazuje zajistit, že všechny osoby, které se na plnění Smlouvy podílejí (bez ohledu na to, zda budou činnosti prováděny Dodavatelem či jeho poddodavateli), jsou vedeny v příslušných registrech, jako například v registru pojištěnců ČSSZ, a mají příslušná povolení k pobytu v ČR.
- 10.7. Dodavatel je dále povinen zajistit, že všechny osoby, které se na plnění Smlouvy podílejí (bez ohledu na to, zda budou činnosti prováděny Dodavatelem či jeho poddodavateli) budou proškoleny z problematiky BOZP, a že jsou vybaveny osobními ochrannými pracovními prostředky dle účinné legislativy, je-li používání osobních ochranných pracovních prostředků s ohledem na předmět plnění Smlouvy vyžadováno. V případě, že Dodavatel (či jeho poddodavatel) bude v rámci řízení zahájeného dle tohoto odstavce Smlouvy orgánem veřejné moci pravomocně uznán vinným ze spáchání přestupku, správního deliktu či jiného obdobného protiprávního jednání, je Dodavatel povinen přijmout nápravná opatření a o těchto, včetně jejich realizace, písemně informovat Objednatele, a to v přiměřené lhůtě stanovené po dohodě s Objednatелеm. Objednatel je oprávněn odstoupit od této Smlouvy, pokud Dodavatel nebo jeho poddodavatel bude orgánem veřejné moci uznán pravomocně vinným ze spáchání přestupku či správního deliktu, popř. jiného obdobného protiprávního jednání, v řízení dle tohoto odstavce Smlouvy.
- 10.8. Dodavatel musí po celou dobu trvání Smlouvy sjednat a dodržovat srovnatelné smluvní podmínky v oblasti rozdělení rizika a smluvních pokut se svými poddodavateli s ohledem na charakter, rozsah a cenu plnění poddodavatele, jako jsou sjednané v této Smlouvě.

- 10.9. Dodavatel se zavazuje po celou dobu trvání Smlouvy zajistit dodržování právních předpisů z oblasti práva životního prostředí, jež naplňuje cíle environmentální politiky související se změnou klimatu, využíváním zdrojů a udržitelnou spotřebou a výrobou, především zákona č. 114/1992 Sb., o ochraně přírody a krajiny, ve znění pozdějších předpisů a zákona č. 17/1992 Sb., o životním prostředí, ve znění pozdějších předpisů.
- 10.10. V případě, že Dodavatel (či jeho poddodavatel) bude v rámci řízení zahájeného orgánem veřejné moci pravomocně uznán vinným ze spáchání přestupku či jiného závažného protiprávního jednání v oblasti práva životního prostředí, je Dodavatel povinen:
- 10.10.1. o této skutečnosti nejpozději do sedmi (7) pracovních dnů písemně informovat Objednatele,
 - 10.10.2. přijmout nápravná opatření k odstranění trvání protiprávního stavu a tento v přiměřené lhůtě odstranit a/nebo učinit prevenční nápravná opatření za účelem zamezení opakování předmětného protiprávního jednání,
 - 10.10.3. písemně informovat Objednatele o opatřeních dle odst. 10.10.2 této Smlouvy, včetně jejich realizace, a to bezodkladně nebo v Objednatelem stanovené lhůtě (bude-li ze strany Objednatele stanovena).
- 10.11. Dodavatel se v rámci svých vnitřních procesů zavazuje k podpoře firemní kultury založené na motivaci pracovníků k zavádění inovativních prvků, procesů či technologií v rámci tzv. best practices.

11. ODPOVĚDNOST ZA VADY, ZÁRUKA

- 11.1. Dodavatel poskytuje záruku, že každá část Plnění má ke dni její akceptace funkční vlastnosti stanovené touto Smlouvou a je způsobilá k použití pro účely stanovené v této Smlouvě nebo v souladu s touto Smlouvou.
- 11.2. Dodavatel poskytuje záruku za jakost každé jednotlivé části poskytovaného dílčího plnění Dodávky hardware od okamžiku její akceptace po dobu třiceti šesti (36) měsíců od akceptace poslední dílčí Dodávky hardware.
- 11.3. Objednatel je oprávněn vady plnění nahlásit Dodavateli kdykoli v průběhu záruční doby bez ohledu na to, kdy je zjistil, aniž by tím byla jeho práva ze záruky či práva z vad jakkoli dotčena.
- 11.4. Doba od zjištění vady do jejího odstranění se do trvání záruční doby nezapočítává.
- 11.5. Plnění má vady, zejména pokud nebylo poskytnuto ve sjednaném druhu, množství a jakosti. Za vady plnění se považují i vady v návodech (manuálech) k použití, dokladech a dokumentech.

- 11.6. V případě, že je dodáno plnění s vadami, či se na plnění vady v záruční době vyskytnou, je Dodavatel povinen vady odstranit opravou, dodáním náhradního plnění, či pokud Objednatel takový požadavek uvede v oznámení vad, přiměřenou slevou z ceny Plnění.
- 11.7. Nároky z vad Plnění se nedotýkají nároku Objednatele na náhradu újmy nebo na smluvní pokutu.

12. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA

- 12.1. Dodavatel prohlašuje, že jakékoli Plnění dle této Smlouvy nebude zatíženo právy třetích osob, ze kterých by pro Objednatele vyplynuly jakékoliv další finanční nebo jiné nároky ve prospěch třetích stran. V opačném případě Dodavatel ponese veškeré důsledky takového porušení práv třetích osob.

Vlastnické právo

- 12.2. V případě, že součástí Plnění Dodavatele podle této Smlouvy jsou věci, které se mají stát vlastnictvím Objednatele, nabývá Objednatel vlastnické právo k těmto věcem dnem předání takového Plnění Objednateli na základě akceptačního protokolu podepsaného oprávněnými osobami obou Smluvních stran. Nebezpečí škody na předaných věcech přechází na Objednatele okamžikem jejich faktického předání do dispozice Objednatele, pokud o takovém předání byl sepsán písemný záznam podepsaný oprávněnými osobami Smluvních stran.
- 12.3. Do okamžiku nabytí vlastnického práva uděluje Dodavatel Objednateli právo dodané zboží užívat v rozsahu a způsobem, jenž vyplývá z účelu této Smlouvy, a to bez vzniku jakýchkoliv dodatečných finančních nároků nad rámec ceny sjednané v této Smlouvě. Užití zboží nezpůsobuje fikci převzetí zboží ani podpisu akceptace.

Základní rozsah licence

- 12.4. Vzhledem k tomu, že součástí Plnění je i plnění, které ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**autorský zákon**“), může naplňovat znaky autorského díla či být považováno za autorské dílo ve smyslu autorského zákona (dále společně jen „**autorská díla**“), je k tomuto plnění poskytována, postupována či zprostředkovávána (dále také společně jen „**poskytování**“) licence či podlicence (dále společně jen „**licence**“) za podmínek sjednaných dále v tomto článku Smlouvy.

- 12.4.1. Objednatel je oprávněn od okamžiku účinnosti poskytnutí licence k autorskému dílu dle odst. 12.4.6 Smlouvy užívat toto autorské dílo k jakémukoliv účelu a v rozsahu, v jakém uzná za nezbytné, vhodné či přiměřené. Pro vyloučení pochybností to znamená, že Objednatel je

oprávněn užívat autorské dílo v neomezeném množstevním a územním rozsahu, a to všemi v úvahu přicházejícími způsoby a s časovým rozsahem omezeným pouze dobou trvání majetkových autorských práv k takovému autorskému dílu.

12.4.2. Objednatel je bez potřeby jakéhokoliv dalšího svolení Dodavatele oprávněn udělit třetí osobě podlicenci k užití autorského díla nebo svoje oprávnění k užití autorského díla třetí osobě postoupit.

12.4.3. Součástí licence je neomezené oprávnění Objednatele provádět jakékoliv modifikace, úpravy, změny autorského díla tvořícího součást dílčího plnění, a to včetně práva Objednatele dle jeho uvážení do autorského díla zasahovat, zapracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob.

12.4.4. Licence k autorskému dílu je poskytována jako nevýhradní. Objednatel není povinen licenci využít.

12.4.5. V případě počítačových programů se licence vztahuje ve stejném rozsahu na autorské dílo ve strojovém i zdrojovém kódu, jakož i k dokumentaci a dalším koncepčním přípravným materiálům, a to i na případné další verze počítačových programů poskytovaných na základě této Smlouvy. Objednatel má právo na předání zdrojového kódu autorského díla, jakož i ostatních částí poskytovaného software, které nejsou autorskými díly.

12.4.6. Licence se uděluje okamžikem akceptace součástí Dílčího plnění, která příslušné autorské dílo obsahuje; do té doby je Objednatel oprávněn autorské dílo užít v rozsahu a způsobem nezbytným k provedení akceptace příslušného Dílčího plnění.

12.4.7. Udělení licence nelze ze strany Dodavatele do doby trvání této Smlouvy vypovědět a její účinnost trvá minimálně po dobu trvání této Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak.

12.4.8. Pro vyloučení veškerých pochybností Smluvní strany výslovně prohlašují, že pokud při poskytování Plnění vznikne činností Dodavatele a Objednatele dílo spoluautorů a nedohodnou-li se Smluvní strany výslovně jinak, Dodavatel k okamžiku vzniku takového díla spoluautorů postoupí Objednateli právo vykonávat majetková autorská práva k dílu spoluautorů a udělí Objednateli souhlas k jakékoliv změně nebo jinému zásahu do díla spoluautorů. Cena za dodání/poskytování Plnění je

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

12.4.9. Dodavatel je povinen postupovat tak, aby udělení licence k autorskému dílu dle této Smlouvy včetně oprávnění udělit podlicenci a souvisejících oprávnění zabezpečil, a to bez újmy na právech třetích osob.

12.4.10. Dodavatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva autorů k autorským dílům, která budou součástí plnění podle této Smlouvy, resp. že má souhlas všech relevantních třetích osob k poskytnutí licence k autorským dílům podle této Smlouvy; toto prohlášení zahrnuje i taková práva, která vytvořením autorského díla teprve vzniknou.

Možnost užití standardního software

12.5. Tzv. proprietární (standardní) software anebo tzv. open source software Dodavatele nebo třetích stran (dále jen „**Standardní software**“), u nějž Dodavatel nemůže udělit Objednateli licenci v rozsahu dle odst. 12.4 této Smlouvy nebo to po něm nelze spravedlivě požadovat, může být součástí Plnění pouze tehdy, kdy vývoj software není hrazen Objednatelem dle této Smlouvy a současně je splněna některá z následujících podmínek:

12.5.1. Jedná se o software, který je v době uzavření Smlouvy prokazatelně užíván v produktivním prostředí nejméně u deseti (10) na sobě nezávislých a vzájemně nepropojených subjektů a jenž je na trhu běžně dostupný, tj. nabízený na území České republiky alespoň třemi (3) na sobě nezávislými a vzájemně nepropojenými subjekty:

12.5.2. pokud jsou tyto subjekty oprávněny takovýto software implementovat, přizpůsobovat požadavkům Objednatele a udržovat; nebo

12.5.3. pokud k takovému software není poskytnutí licence v rozsahu dle odst. 12.4 této Smlouvy účelné a nebrání dalšímu rozvoji plnění ze strany Objednatele (zejména vývojový software, databázový software, kancelářský software, operační systém aj.).

Takový Standardní software musí být plně oddělitelný od předmětného Dílčího plnění. Dodavatel je povinen poskytnout Objednateli o skutečnostech dle tohoto odstavce Smlouvy písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

12.5.4. Jedná se o software, který je veřejnosti poskytován a bude Objednateli poskytnut zdarma, včetně detailně komentovaných zdrojových kódů a práva software měnit. Dodavatel je povinen poskytnout Objednateli

o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

12.5.5. Jedná se o software, k němuž Dodavatel Objednateli nejpozději současně s jeho akceptací ze strany Objednatele poskytne nebo zprostředkuje poskytnutí úplných komentovaných zdrojových kódů a bezpodmínečné právo provádět jakékoliv modifikace, úpravy, změny takového software a dle svého uvážení do něj zasahovat, zapracovávat ho do dalších autorských děl, zařazovat ho do děl souborných či do databází apod., a to i prostřednictvím třetích osob. Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

12.5.6. Jedná se o software, (i) který je integrální součástí hardware dodávaného jako část plnění Smlouvy nebo (ii) který nad takovým hardware poskytuje pouze abstrakční vrstvu pro programování aplikací, vše za podmínky, že spouštění takového software je od výrobce příslušného hardware předepsáno pro jeho korektní fungování a zároveň se jedná o software, k němuž není poskytnutí licence v rozsahu dle odst. 12.4 této Smlouvy účelné a nebrání dalšímu rozvoji plnění ze strany Objednatele. Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

12.5.7. Jedná se o software, u kterého Dodavatel poskytne s ohledem na jeho (i) marginální význam, (ii) nekomplikovanou propojitelnost či (iii) oddělitelnost a nahraditelnost v systémech Objednatele bez nutnosti vynakládání výraznějších prostředků, písemnou garanci, že další plnění jinou osobou než Dodavatelem je možné provádět bez toho, aby tím byla dotčena práva autorů takového software, neboť nebude nutné zasahovat do zdrojových kódů takového software anebo proto, že případné nahrazení takového software nebude představovat výraznější komplikaci a náklad na straně Objednatele. Dodavatel je povinen poskytnout Objednateli o této skutečnosti písemné prohlášení a na výzvu Objednatele tuto skutečnost prokázat.

12.6. V případě že Dodavatel poruší povinnosti vyplývající z užití Standardního software dle odst. 12.5 této Smlouvy, nepředloží Objednateli příslušné prohlášení dle odst. 12.5 této Smlouvy či nejpozději do jednoho (1) měsíce na výzvu Objednatele relevantní skutečnosti neprokáže, je Objednatel oprávněn požadovat úhradu smluvní pokuty ve výši 2.000.000,- Kč za každý jednotlivý případ a náhradu škody v plné výši, a dále bezodkladné zajištění nápravy, a to včetně náhrady příslušného software.

Minimální rozsah licence

- 12.7. V případě užití Standardního software splňujícího podmínky dle odst. 12.5 této Smlouvy postačí, na rozdíl od licence ke zbývajícím částem Plnění udělované dle odst. 12.4 této Smlouvy, aby udělená licence k takovému Standardnímu software zahrnovala nevýhradní oprávnění užít jej jakýmkoli způsobem nejméně po dobu trvání této Smlouvy, na území České republiky a v množstevním rozsahu odpovídajícím alespoň množstevnímu rozsahu licence, který je objektivně nezbytný pro pokrytí potřeb Objednatele, a to včetně práva Objednatele do Standardního software zasahovat a dalších specifických oprávnění Objednatele, pokud tak stanoví příslušné ustanovení odst. 12.5 této Smlouvy.
- 12.8. Užití Standardního software v souladu s účelem této Smlouvy a dle pokynů Objednatele nesmí vést k povinnosti zveřejnit zdrojový kód jakékoli části Plnění poskytnutých dle této Smlouvy.
- 12.9. Dodavatel je povinen zajistit splnění všech povinností souvisejících sužitím Standardního software, včetně zejména označení autora, uvedení informace o jeho licenčních podmínkách apod.
- 12.10. V případě výpovědi či odstoupení od Smlouvy se Dodavatel zavazuje nabídnout Objednateli právo užívat Standardní software v rozsahu, v jakém je to nezbytné pro řádné užívání plnění dle této Smlouvy. Tím není dotčeno právo Objednatele pořídit Standardní software i od třetí osoby bez ohledu na licence pořízené dříve Dodavatelem. V případě využití tohoto přednostního práva se Dodavatel zavazuje, že právo užívat Standardní software dle tohoto odstavce Smlouvy nabídne Objednateli za běžných tržních podmínek a bude vycházet z účetní hodnoty licencí, které pořídil.
- 12.11. Nelze-li to na Dodavateli spravedlivě požadovat a není-li to v rozporu s ustanoveními odst. 12.5 této Smlouvy, nemusí být Objednateli ke Standardnímu softwaru předány zdrojové kódy a stejně tak nemusí být Objednateli poskytnuto právo do Standardního software zasahovat, vždy však musí být předána kompletní uživatelská, administrátorská, bezpečnostní a provozní dokumentace.
- 12.12. Dodavatel se zavazuje samostatně zdokumentovat veškeré využití Standardního software v rámci plnění a předložit Objednateli ucelený přehled využitého Standardního software, jehož součástí budou licenční podmínky takového Standardního software, seznam jeho alternativních dodavatelů, a výčet povinností vyplývajících z užití takového Standardního software. Tento přehled je Dodavatel povinen předložit Objednateli vždy do tří (3) pracovních dnů po akceptaci Dílčího plnění, v jehož rámci Dodavatel využil Standardní software a dále vždy do jednoho (1) měsíce od doručení výzvy Objednatele, kterou může Objednatel učinit kdykoli, nejpozději však do dvou (2) let od skončení účinnosti Smlouvy z jakéhokoli důvodu.

- 12.13. Jestliže jsou s užitím Standardního software spojeny jednorázové poplatky, je Dodavatel povinen v rámci ceny plnění řádně uhradit všechny tyto poplatky po dobu trvání této Smlouvy.

Přechod práv, licenční odměna a garance rozsahu licence

- 12.14. Práva získaná v rámci plnění této Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Dodavatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Dodavatelem Objednateli.
- 12.15. Smluvní strany se pro vyloučení pochybností výslovně dohodly, že veškerá data, která vzniknou v rámci plnění této Smlouvy, náležejí Objednateli, a to bez ohledu na to, zda případně budou v rámci plnění ze strany Dodavatele upravována.
- 12.16. Bez ohledu na formu uzavření licenční smlouvy platí, že Dodavatel je vždy povinen zajistit poskytnutí licence dle podmínek stanovených Smlouvou, a to bez ohledu na případný rozdílný obsah standardních licenčních podmínek vykonavatele majetkových práv k takovým autorským dílům.

13. OPRÁVNĚNÉ OSOBY

- 13.1. Každá ze Smluvních stran jmenuje oprávněnou osobu, popř. zástupce oprávněné osoby. Oprávněné osoby budou zastupovat Smluvní stranu ve smluvních, obchodních a technických záležitostech souvisejících s plněním této Smlouvy.
- 13.2. Oprávněné osoby jsou oprávněny jménem Smluvních stran provádět zejména veškeré úkony v rámci realizace Smlouvy, zastupovat Smluvní strany ve změnovém řízení a připravovat dodatky ke Smlouvě pro jejich písemné schválení osobám oprávněným zavazovat Smluvní strany (statutárním orgánům), nebo jejich zplnomocněným zástupcům.
- 13.3. Oprávněné osoby nejsou zmocněny k jednání, jež by mělo za přímý následek změnu této Smlouvy nebo jejího předmětu.
- 13.4. Jména oprávněných osob jsou uvedena v **Příloze č. 6** této Smlouvy a jejich role stanoví tato Smlouva.
- 13.5. Smluvní strany jsou oprávněny změnit oprávněné osoby, jsou však povinny na takovou změnu druhou Smluvní stranu písemně upozornit ve lhůtě tří (3) dnů. Zmocnění zástupce oprávněné osoby musí být písemné s uvedením rozsahu zmocnění.
- 13.6. Smluvní strany tímto prohlašují, že budou jako samostatní správci zpracovávat osobní údaje fyzických osob jednajících na straně druhé Smluvní strany (zejména pokud se jedná o identifikační a kontaktní údaje oprávněných osob) a případně dalších osob podílejících se na plnění Smlouvy (jako subjekty údajů) pro účely plnění Smlouvy, interní evidence správce a ochranu jeho práv, dodržování zákonných povinností vztahujících se ke správci.

- 13.7. Právní základ pro takové zpracování osobních údajů je oprávněný zájem správce na řádném plnění uzavřené Smlouvy, oprávněný zájem správce na evidenci smluv, ve kterých je správce smluvní stranou, a na ochraně jeho práv, nutnost plnění zákonných povinností, kterým správce podléhá, zejména v oblasti daňových a účetních zákonů.
- 13.8. Osobní údaje musí být uchovávány po dobu trvání této Smlouvy a plnění povinností z ní vyplývajících a po dobu nezbytnou k plnění právních povinností Smluvních stran.
- 13.9. Obě Smluvní strany se zavazují informovat své zaměstnance a dodavatele o zpracování jejich osobních údajů jinou Smluvní stranou na základě této Smlouvy bez zbytečného odkladu.

14. OCHRANA INFORMACÍ A OSOBNÍCH ÚDAJŮ

- 14.1. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:
- 14.1.1. si mohou vzájemně vědomě nebo opomenutím poskytnout informace, které budou považovány za důvěrné (dále jen „**Důvěrné informace**“);
 - 14.1.2. mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé Smluvní strany nebo i jejím opomenutím přístup k Důvěrným informacím druhé Smluvní strany.
- 14.2. Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě důvěrné informace, které při plnění této Smlouvy získala od druhé Smluvní strany.
- 14.3. Třetími osobami podle odst. 14.2 Smlouvy nejsou:
- 14.3.1. zaměstnanci Smluvních stran a osoby v obdobném postavení;
 - 14.3.2. orgány Smluvních stran a jejich členové;
 - 14.3.3. ve vztahu k Důvěrným informacím Objednatele poddodavatelé Dodavatele;
 - 14.3.4. ve vztahu k Důvěrným informacím Dodavatele externí poskytovatelé Objednatele, a to i potenciální;
- za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeném s plněním dle této Smlouvy, Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny Smluvními stranám v této Smlouvě.
- 14.4. Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající Smluvní strany a přijímající Smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě Smluvní strany zavazují neduplikovat žádným způsobem Důvěrné informace druhé Smluvní strany, nepředat je

třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Obě Smluvní strany se zároveň zavazují nepoužít Důvěrné informace druhé Smluvní strany jinak než za účelem plnění této Smlouvy.

- 14.5. Nedohodnou-li se Smluvní strany výslovně písemnou formou jinak, jsou Důvěrné informace implicitně všechny informace, které jsou anebo by mohly být součástí obchodního tajemství, tj. například, ale nejenom, popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající Smluvní stranou by předávající straně mohlo způsobit újmu.
- 14.6. Bez ohledu na výše uvedená ustanovení jsou veškeré informace vztahující se k předmětu této Smlouvy a příslušné dokumentaci výlučně Důvěrnými informacemi Objednatele a Dodavatel je povinen tyto informace chránit v souladu s touto Smlouvou. Dodavatel přitom bere na vědomí, že povinnost ochrany těchto informací podle tohoto čl. 14 Smlouvy se vztahuje pouze na Dodavatele.
- 14.7. Pokud jsou Důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médii), je předávající Smluvní strana povinna upozornit přijímající Smluvní stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce nebo přední straně média. Absence takového upozornění však nezpůsobuje zánik povinnosti ochrany takto poskytnutých informací.
- 14.8. Bez ohledu na výše uvedená ustanovení se za Důvěrné informace nepovažují informace, které:
- 14.8.1. se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající Smluvní strany či právních předpisů;
 - 14.8.2. mají být zpřístupněny Objednatelem na základě zákona, například zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, či jiného právního předpisu včetně práva EU nebo závazného rozhodnutí oprávněného orgánu veřejné moci, a Smluvní strany si v takovém případě poskytnou nezbytnou součinnost ke splnění takové zákonné povinnosti;
 - 14.8.3. měla přijímající Smluvní strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly

- předmětem jiné, dříve mezi Smluvními stranami uzavřené smlouvy o ochraně informací;
- 14.8.4. jsou výsledkem postupu, při kterém k nim přijímající Smluvní strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany;
- 14.8.5. po podpisu této Smlouvy poskytne přijímající straně třetí osoba, jež není omezena v takovém nakládání s informacemi;
- 14.8.6. jsou obsažené ve Smlouvě a jsou uveřejněné dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „**ZRS**“) a v souladu se ZZVZ.
- 14.9. Porušením povinnosti mlčenlivosti Smluvní stranou jsou též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v odst. 14.3 Smlouvy, které daná Smluvní strana poskytla Důvěrné informace druhé Smluvní strany.
- 14.10. Poruší-li Dodavatel povinnosti vyplývající z této Smlouvy ohledně ochrany důvěrných informací, je povinen zaplatit Objednateli smluvní pokutu ve výši 100.000,- Kč za každé takové porušení povinnosti.
- 14.11. Ukončení účinnosti této Smlouvy z jakéhokoliv důvodu se nedotkne ustanovení tohoto čl. 14 Smlouvy a jejich účinnost přetrvá i po ukončení účinnosti této Smlouvy.
- 14.12. Dodavatel dále výslovně prohlašuje a bere na vědomí, že tato Smlouva nepředstavuje jeho obchodní tajemství ani neobsahuje jeho Důvěrné informace a souhlasí s tím, aby tato Smlouva byla v plném rozsahu zveřejněna v souladu se zákonnými povinnostmi Objednatele.
- 14.13. S ohledem na předmět této Smlouvy Smluvní strany předpokládají, že Dodavatel může během poskytování Plnění zpracovávat osobní údaje nebo zvláštní kategorie osobních údajů (citlivé údaje) (dále společně jen „**osobní údaje**“).
- 14.14. Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit osobní údaje vyplývající z této Smlouvy a též z příslušných právních předpisů, zejména povinnosti vyplývající z nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), CELEX: 32016R0679 (dále jen „**Nařízení GDPR**“).
- 14.15. Nedílnou součástí Smlouvy je tak i ujednání o zpracování osobních údajů mezi Objednatелеm jako správcem a Dodavatelem jako zpracovatelem, uvedené v **Příloze č. 8** této Smlouvy.

- 14.16. Zpracování osobních údajů bude Dodavatel provádět jako součást poskytování Plnění dle této Smlouvy, kdy odměna Dodavatele za zpracování osobních údajů je zahrnuta v ceně za Plnění.
- 14.17. Zpracování osobních údajů bude ze strany Dodavatele probíhat po dobu účinnosti Smlouvy. Povinnosti Dodavatele týkající se ochrany osobních údajů se Dodavatel zavazuje plnit po celou dobu účinnosti Smlouvy, pokud z ustanovení Smlouvy nevyplývá, že mají trvat i po zániku její účinnosti.

15. VZÁJEMNÁ KOMUNIKACE

- 15.1. Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím oprávněných osob vymezených v **Příloze č. 6** této Smlouvy, statutárních orgánů Smluvních stran, popř. jimi písemně pověřených pracovníků.
- 15.2. Všechna oznámení mezi Smluvními stranami, která se vztahují k této Smlouvě, nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé Smluvní straně doručena buď osobně nebo doporučeným dopisem či jinou formou registrovaného poštovního styku na adresu uvedenou na titulní stránce této Smlouvy, není-li stanoveno nebo mezi Smluvními stranami dohodnuto jinak. Nemá-li komunikace dle předchozí věty mít vliv na platnost a účinnost Smlouvy, připouští se též doručení prostřednictvím e-mailu na adresy uvedené v **Příloze č. 6** této Smlouvy. Dodavatel je oprávněn komunikovat s Objednatelem prostřednictvím datové schránky.
- 15.3. Ukládá-li Smlouva doručit některý dokument v písemné podobě, může být doručen buď v tištěné podobě nebo v elektronické (digitální) podobě jako dokument aplikace MS Word verze 2003 nebo vyšší, MS Excel 2003 nebo vyšší či PDF (verze založena na specifikaci ISO 32000-1:2008) na dohodnutém médiu.
- 15.4. Smluvní strany se zavazují, že v případě změny své poštovní adresy, nebo e-mailové adresy budou o této změně druhou Smluvní stranu informovat nejpozději do tří (3) dnů.
- 15.5. Dodavatel se zavazuje ve lhůtě pěti (5) pracovních dnů ode dne doručení odůvodněné písemné žádosti Objednatele o výměnu oprávněné osoby Dodavatele podílející se na plnění této Smlouvy, s níž Objednatel nebyl z jakéhokoliv důvodu spokojen, nahradit tuto osobu jinou vhodnou osobou s odpovídající kvalifikací.

16. NÁHRADA ÚJMY

- 16.1. Každá ze Smluvních stran nese odpovědnost za způsobenou újmu v rámci platných právních předpisů a této Smlouvy. Obě Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.
- 16.2. Žádná ze Smluvních stran neodpovídá za újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany.

V případě, že Objednatel poskytl Dodavateli chybné zadání a Dodavatel s ohledem na svou povinnost poskytovat Plnění s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.

- 16.3. Žádná ze Smluvních stran není odpovědná za újmu a není ani v prodlení, pokud k tomuto došlo výlučně v důsledku prodlení s plněním závazků druhé Smluvní strany nebo v důsledku překážek vylučujících povinnost k náhradě újmy ve smyslu § 2913 odst. 2 OZ (dále jen „**vyšší moc**“). Pro uplatnění vyšší moci se použijí následující pravidla:

16.3.1. Dodavatel bez zbytečného odkladu uvědomí Objednatele písemně o takových překážkách a jejich příčině. Pokud není jinak stanoveno písemně Objednatelem, bude Dodavatel pokračovat v realizaci svých závazků vyplývajících ze smluvního vztahu v rozsahu svých nejlepších možností a schopností a bude hledat alternativní prostředky pro realizaci té části plnění, které brání vyšší moc, přičemž však nebude ve vztahu k této části plnění v prodlení. Pokud by podmínky vyšší moci trvaly déle než 60 dní, je Objednatel oprávněn od Smlouvy nebo její části odstoupit.

16.3.2. Pro účely této Smlouvy je vyšší mocí událost, která je mimo kontrolu Smluvní strany, nastala po podpisu této Smlouvy, kterou nebylo možno předvídat a ke které došlo bez zavinění Smluvní strany, pokud nebyla způsobena její chybou či nedbalostí.

16.3.3. Událostmi způsobujícími vyšší moc jsou zejména živelní pohromy, přírodní katastrofy, jakákoliv embargo, občanské války, revoluce, povstání, válečné konflikty, teroristické útoky, nepokoje, epidemie nebo karanténní omezení. Živelními pohromami jsou zejména požár, úder blesku, povodeň nebo záplava, vichřice nebo krupobití, sesuv nebo zřícení lavin, skal, zemin nebo kamení.

16.3.4. Události vylučující odpovědnost Dodavatele výslovně nejsou jakákoliv prodlení s plněním povinností smluvních partnerů Dodavatele, stávka zaměstnanců Dodavatele a jeho smluvních partnerů, jakož i insolvence, předlužení, konkurs, reorganizace, likvidace či jiná obdobná událost týkající se Dodavatele nebo jakéhokoliv smluvního partnera Dodavatele a exekuce majetku Dodavatele nebo jakéhokoliv smluvního partnera Dodavatele, a to s výjimkou případů, kdy by se na smluvní partnery Dodavatele uplatnily některé z případů dle odst. 16.3.3 Smlouvy.

16.3.5. Smluvní strany nejsou ve vztahu k té části plnění, které brání vyšší moc, v prodlení pouze po dobu existence takové okolnosti vylučující povinnost k náhradě újmy nebo trvání jejích následků a pouze ve vztahu

k povinnosti nebo povinnostem Smluvní strany přímo nebo bezprostředně ovlivněných takovou okolností.

16.3.6. Smluvní strany jsou povinny se neprodleně o všech těchto okolnostech vylučujících odpovědnost informovat a prokázat, že je překážka mimo kontrolu dotčené Smluvní strany, že ji nebylo možné v době uzavření Smlouvy rozumně předvídat a že účinky překážky nemohly být rozumně odvráceny nebo překonány. Nedojde-li k oznámení neprodleně, nastávají účinky dle tohoto odst. 16.3 Smlouvy až doručením oznámení dle tohoto odstavce.

16.3.7. Smluvní strany jsou dále povinny vstoupit do jednání ohledně řešení vzniklé situace. Objednatel ani Dodavatel nejsou oprávněni takto vzniklé situace jakkoliv zneužít ve svůj prospěch a jsou povinni v dobré víře usilovat o dosažení přijatelného řešení pro Smluvní strany v co nejkratší době. V případě porušení této povinnosti spolupracovat kteroukoliv Smluvní stranou, je tato Smluvní strana v prodlení s plněním svých povinností dle této Smlouvy.

16.3.8. V případě, že nedojde k dohodě Smluvních stran, termíny plnění jednotlivých povinností podle Smlouvy dotčené okolností vylučující odpovědnost se prodlužují o dobu, po kterou okolnost vylučující odpovědnost trvala.

16.3.9. Odpovědnost nevylučuje událost, která vznikla teprve v době, kdy povinná Smluvní strana byla v prodlení s plněním své povinnosti, či vznikla z jejích hospodářských poměrů.

16.4. Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé překážky vylučující povinnost k náhradě újmy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání překážek vylučujících povinnost k náhradě újmy. Každá ze Smluvních stran je oprávněna požadovat náhradu újmy v plném rozsahu i v případě, že se jedná o porušení povinnosti, na kterou se dle této Smlouvy vztahuje smluvní pokuta nebo sleva z ceny.

16.5. Smluvní strany se dohodly, že omezují právo na náhradu újmy, která může při plnění této Smlouvy jedné smluvní straně vzniknout, a to na celkovou částku odpovídající 100 % z maximální ceny plnění dle odst. 9.4 Smlouvy. Ustanovení § 2898 Občanského zákoníku však tímto není dotčeno.

16.6. Případná náhrada újmy bude zaplacená v měně platné na území České republiky, přičemž pro propočet na tuto měnu je rozhodný kurs České národní banky ke dni vzniku újmy.

- 16.7. Každá ze Smluvních stran je oprávněna požadovat náhradu újmy i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta nebo sleva z ceny, a to v celém rozsahu nebo slevy z ceny dle této Smlouvy.

17. SANKCE

- 17.1. Smluvní strany se dohodly, že:

- 17.1.1. V případě, že Dodavatel je v prodlení s provedením Dodávky hardware a Podpory výrobce dle Harmonogramu, je Dodavatel povinen uhradit a Objednatel je oprávněn po Dodavateli požadovat uhrazení smluvní pokuty ve výši 0,1 % z celkové nabídkové ceny za Dodávku hardware a Podporu výrobce uvedené v nabídce Dodavatele, a to za každý započatý den prodlení.
- 17.1.2. V případě, že dojde k porušení povinnosti dle odst. 5.7 této Smlouvy, může Objednatel požadovat po Dodavateli jednorázovou smluvní pokutu ve výši 500.000,- Kč. Současně bude mít Objednatel právo odstoupit od této Smlouvy z důvodu podstatného porušení Smlouvy.
- 17.1.3. V případě, že Dodavatel nesplní povinnost dle odst. 5.4 Smlouvy do pěti (5) pracovních dnů od doručení žádosti Objednatele o předložení potvrzení výrobce o určení dodaného zboží pro evropský trh, případně jiného dokladu výrobce, prokazujícího pro dodaná zařízení provozovaná na území ČR poskytnutí plné podpory a záruky výrobce při řešení technických problémů, může Objednatel požadovat po Dodavateli jednorázovou smluvní pokutu ve výši 500.000,- Kč. Současně bude mít Objednatel právo odstoupit od této Smlouvy z důvodu podstatného porušení Smlouvy.
- 17.1.4. V případě porušení povinnosti dle odst. 6.3 Smlouvy, může Objednatel požadovat po Dodavateli smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý případ porušení povinnosti.
- 17.1.5. V případě, že v průběhu záruční doby Objednatel zjistí, že vlastnosti (zejm. technické parametry) hardware jsou prokazatelně v rozporu s touto Smlouvou (nesplňují minimální požadované parametry uvedené v Zadávací dokumentaci), může Objednatel požadovat po Dodavateli jednorázovou smluvní pokutu ve výši 500.000,- Kč. Současně bude mít Objednatel právo odstoupit od této Smlouvy z důvodu podstatného porušení Smlouvy.
- 17.1.6. Pro případ prokazatelného porušení povinnosti Dodavatele dle čl. 10 Smlouvy vzniká Objednateli, nárok na smluvní pokutu ve výši 5.000,- Kč za každé jednotlivé porušení.

17.1.7. Za porušení povinnosti uvedené v odst. 10.5 této Smlouvy, tj. porušení povinnosti Dodavatele mít po celou dobu platnosti Smlouvy sjednáno pojištění odpovědnosti za škodu způsobenou v souvislosti s výkonem podnikatelské činnosti v rozsahu touto Smlouvou, uhradí Dodavatel smluvní pokutu ve výši 100.000,- Kč.

17.2. Smluvní strany se dále dohodly, že:

17.2.1. V případě, že Dodavatel bude k poskytování Plnění využívat poddodavatele nebo členy realizačního týmu v rozporu s ustanoveními odst. 3.4 nebo odst. 3.5 této Smlouvy, vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 50.000,- Kč za každý jednotlivý případ takového porušení Smlouvy.

17.2.2. V případě porušení jakékoliv povinnosti Dodavatele dle článku čl. 20 Smlouvy vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 100.000,- Kč za každý jednotlivý případ porušení.

17.2.3. Za porušení povinnosti mlčenlivosti specifikované v čl. 14 této Smlouvy uhradí Dodavatel Objednateli částku 50.000,- Kč za každý jednotlivý případ porušení této povinnosti.

17.3. Dodavatel je povinen zajistit, aby plněním této Smlouvy nedošlo k porušení právních předpisů a rozhodnutí upravujících mezinárodní sankce, kterými jsou Česká republika nebo Objednatel vázáni. Dodavatel je neprodleně povinen informovat Objednatele o skutečnostech, jakkoliv relevantních pro posouzení naplnění povinností uvedených ve větě první tohoto bodu Smlouvy. Současně platí, že:

17.3.1. Objednatel je oprávněn od této Smlouvy či její části odstoupit, pokud zjistí, že na Dodavatele či Dodavatelem ovládané osoby dopadají, přímo či zprostředkovaně, mezinárodní sankce dle příslušných právních předpisů a rozhodnutí, kterými jsou Česká republika nebo Objednatel vázáni.

17.3.2. Pokud takové sankce dopadají na jakoukoli osobu, kterou Dodavatel používá k plnění Smlouvy, včetně poddodavatelů, je Dodavatel povinen o takové skutečnosti nejpozději následující pracovní den poté, co ji zjistí, informovat Objednatele a do čtrnácti (14) dní od výzvy Objednatele je povinen zjednat nápravu a takovou osobu nahradit, přičemž pokud tak neučiní, je Objednatel oprávněn od Smlouvy či její části odstoupit.

17.3.3. Pokud Dodavatel poruší svou informační povinnost upravenou v 17.3 věta druhá Smlouvy nebo odst. 17.3.2 Smlouvy, je povinen uhradit Objednateli smluvní pokutu ve výši 0,5 % z ceny Plnění v Kč bez DPH za každý započatý den porušení uvedené povinnosti.

- 17.4. Smluvní pokuty a/nebo úroky z prodlení jsou splatné třicátý (30.) den ode dne doručení písemné výzvy oprávněné Smluvní strany k jejich úhradě povinnou Smluvní stranou, není-li ve výzvě uvedena lhůta delší.
- 17.5. Není-li dále stanoveno jinak, zaplacení jakékoliv sjednané smluvní pokuty nezbavuje povinnou Smluvní stranu povinnosti splnit své závazky.
- 17.6. Zaplacením smluvní pokuty není dotčeno právo Objednatele na náhradu újmy v celém rozsahu. Výše smluvních pokut se do výše náhrady újmy nezapočítává.

18. ZMĚNOVÉ ŘÍZENÍ

- 18.1. Kterákoliv ze Smluvních stran je v průběhu trvání této Smlouvy oprávněna písemně navrhnout změny specifikace Plnění. V případě, že změnu specifikace navrhne Objednatel, je Dodavatel povinen vynaložit veškeré úsilí k tomu, aby změnu specifikace přijal. Objednatel není povinen přijmout změnu specifikace navrhovanou Dodavatelem.
- 18.2. Dodavatel se na písemnou výzvu Objednatele zavazuje do deseti (10) pracovních dnů vyhodnotit důsledky navržených změn specifikace Plnění, které budou zahrnovat hodnocení dopadů těchto změn na cenu a rozsah Plnění, dohodnuté termíny plnění, rozsah potřebné součinnosti a jakékoliv další relevantní aspekty smluvního vztahu (dále jen „**Hodnocení důsledků**“). Pokud si vypracování Hodnocení důsledků vyžádá dodatečné náklady nebo pokud by jeho vypracování mohlo mít negativní dopad na plnění závazků Dodavatele dle této Smlouvy, vypracuje Dodavatel Hodnocení důsledků na základě písemné dohody s Objednatelem o úhradě nákladů na vypracování Hodnocení důsledků a o úpravě dalších smluvních podmínek, kterých se vypracování Hodnocení důsledků může dotknout.
- 18.3. Jakékoliv změny specifikace Plnění dle Smlouvy musí být dohodnuty formou písemného dodatku k této Smlouvě podle odst. 22.1 Smlouvy, kterým dojde k úpravě smluvních podmínek v souladu s Hodnocením důsledků, není-li touto Smlouvou stanoveno jinak.
- 18.4. Jakékoliv změny technické specifikace Plnění uvedené v **Příloze č. 1** Smlouvy nebo Specifikace Provozní podpory uvedené v **Příloze č. 3** Smlouvy musí být sjednány v souladu s příslušnými právními předpisy včetně ZZVZ.

19. PLATNOST A ÚČINNOST SMLOUVY

- 19.1. Tato Smlouva je platná dnem připojení platného uznávaného elektronického podpisu dle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, do této Smlouvy a všech jejích jednotlivých příloh, nejsou-li součástí jediného elektronického dokumentu (tj. všech samostatných souborů tvořících v souhrnu Smlouvu), oběma Smluvními stranami.

- 19.2. Tato Smlouva nabývá účinnosti uveřejněním v registru smluv dle ZRS. Smluvní strany výslovně sjednávají, že uveřejnění této Smlouvy v registru smluv zajistí Objednatel.
- 19.3. Tato Smlouva se uzavírá na dobu určitou, a to na dobu třiceti šesti (36) měsíců ode dne zahájení poskytování Podpory výrobce.
- 19.4. Každá Smluvní strana je oprávněna odstoupit od této Smlouvy z důvodů stanovených touto Smlouvou.
- 19.5. Objednatel je oprávněn odstoupit od této Smlouvy v případě, že:
- 19.5.1. Dodavatel opakovaně (nejméně dvakrát) v průběhu jednoho kalendářního měsíce poskytne vadné Plnění, které způsobí nebo mohou reálně způsobit výpadek IT infrastruktury Objednatele či jeho podstatné části;
 - 19.5.2. Dodavatel je v prodlení s plněním svých povinností déle než patnáct (15) dní a nezjedná nápravu ani do deseti (10) dnů ode dne doručení písemného oznámení Objednatele o takovém prodlení;
 - 19.5.3. dojde k porušení povinnosti ochrany důvěrných informací, ochrany osobních údajů nebo povinností kybernetické bezpečnosti dle této Smlouvy ze strany Dodavatele;
 - 19.5.4. Dodavatel neoznámí změnu člena realizačního týmu uvedeného v **Příloze č. 6** této Smlouvy Objednateli postupem dle odst. 3.4 této Smlouvy; nebo
 - 19.5.5. Dodavatel předem neoznámí Objednateli jakoukoliv změnu osoby poddodavatele nebo zvětšení rozsahu plnění svěřeného poddodavateli ve smyslu odst. 3.5 Smlouvy, nebo k takovéto změně Objednatel nedá předem souhlas dle téhož odstavce.
- , přičemž však není Objednatel oprávněn odstoupit v části Smlouvy týkající se Dodávky hardware a/nebo Podpory výrobce, pokud již Dodavatel prokazatelně provedl objednávku hardware u výrobce a případně také objednávku Podpory výrobce. Objednatel je však oprávněn odstoupit také od Dodávky hardware a/nebo Podpory výrobce v případě porušení podmínek dle odst. 5.4 a 5.7 této Smlouvy.
- 19.6. Objednatel je dále oprávněn bez jakýchkoliv sankcí písemně odstoupit od této Smlouvy, pokud:
- 19.6.1. bylo příslušným orgánem vydáno pravomocné rozhodnutí zakazující plnění této Smlouvy;
 - 19.6.2. na majetek Dodavatele je prohlášen úpadek, Dodavatel sám podá dlužnický návrh na zahájení insolvenčního řízení nebo insolvenční návrh

je zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení;

19.6.3. Dodavatel ztratí příslušného oprávnění poskytovat Plnění dle odst. 1.2.3 Smlouvy;

19.6.4. Dodavatel vstoupí do likvidace; nebo

19.6.5. proti Dodavateli je zahájeno trestní stíhání pro trestný čin podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů.

19.7. Objednatel je oprávněn od Smlouvy odstoupit rovněž v případě, pokud mu nebudou přiděleny rozpočtové prostředky na financování předmětu plnění dle Smlouvy.

19.8. Dodavatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než šedesát (60) dnů, pokud Objednatel nezjedná nápravu ani v dodatečně přiměřené lhůtě, kterou mu k tomu Dodavatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než patnáct (15) dnů od doručení takovéto výzvy.

19.9. Účinky odstoupení od Smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé Smluvní straně.

19.10. Objednatel je oprávněn tuto Smlouvu písemně vypovědět (a to i částečně) bez udání důvodů, a to s tří (3) měsíční výpovědní dobou, která uplyne ke konci měsíce následujícího po měsíci doručení písemné výpovědi Dodavateli. Tuto výpověď nebo částečnou výpověď je Objednatel oprávněn učinit kdykoliv po dobu trvání této Smlouvy.

19.11. Dodavatel je oprávněn tuto Smlouvu písemně vypovědět (pouze jako celek) bez udání důvodů, a to s výpovědní dobou šesti (6) měsíců, počítáno od prvního dne měsíce následujícího po měsíci doručení písemné výpovědi Objednateli.

19.12. Ukončením doby trvání této Smlouvy, a to i předčasným ukončením, nejsou dotčena ustanovení Smlouvy týkající se licencí, záruk, práv z vady, povinnosti nahradit újmu a povinnosti hradit smluvní pokuty, ustanovení o ochraně Důvěrných informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po ukončení doby trvání této Smlouvy.

19.13. Ukončením doby trvání této Smlouvy není dotčeno vzájemné plnění, pokud bylo řádně poskytnuto, ani práva a nároky z takových plnění vyplývající. V případě, kdy by však Objednatel odstoupil od Smlouvy z důvodu takového porušení smluvní povinnosti Dodavatele, že se plnění Dodavatele stalo pro Objednatele nepotřebným, bude toto plnění Dodavateli vráceno a ten bude povinen vrátit Objednateli zaplacenou cenu.

20. KYBERNETICKÁ BEZPEČNOST

20.1. Není-li v této Smlouvě nebo v souladu s touto Smlouvou stanoveno jinak, Dodavatel tímto bere na vědomí, že:

20.1.1. Objednatel je během trvání této Smlouvy správcem informačních systémů kritické informační infrastruktury dle § 3 písm. c) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB“), správcem komunikačního systému kritické informační infrastruktury dle § 3 písm. d) ZKB a správcem významných informačních systémů dle § 3 písm. e) ZKB. Dodavatel dále tímto bere na vědomí, že poskytnutí Plnění specifikovaných v čl. 3 této Smlouvy je prováděno na aktivech systémů kritické informační infrastruktury a aktivech významných informačních systému.

20.1.2. Objednatel tímto informuje Dodavatele, že jej vyhodnotil a eviduje jej jako významného dodavatele 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), ve znění pozdějších předpisů (dále jen „VKB“). V případě, že se Objednatel dále stane správcem některého ze systému ve smyslu odst. 20.1.1 Smlouvy až během trvání Smlouvy, zavazuje se Dodavatele o uvedeném bez zbytečného odkladu informovat, pokud jej bude považovat za významného dodavatele ve vazbě na dotčený systém a bude jej takto evidovat.

20.2. Smluvní strany potvrzují, že rozsah zapojení Dodavatele na zajištění bezpečnosti aktiv informačních a komunikačních systémů kritické informační infrastruktury a aktiv významných informačních systému je určen předmětem této Smlouvy.

20.3. Dodavatel je povinen v rozsahu plnění této Smlouvy naplnit všechny bezpečnostní požadavky uvedené v **Příloze č. 9** této Smlouvy (dále jen „**Kybernetické požadavky**“).

20.4. Dodavatel umožní Objednateli v roční periodě po dobu trvání této Smlouvy a jeden (1) rok po ukončení trvání této Smlouvy provedení zákaznického auditu (kontroly):

20.4.1. jehož rozsah bude ohraničen využíváním ICT prostředků Dodavatele pro potřeby plnění této Smlouvy a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Dodavatele; a

20.4.2. jehož předmětem bude naplnění Kybernetických požadavků a vyhodnocení rizik dle čl. 3 **Přílohy č. 9** této Smlouvy.

- 20.5. Objednatel je oprávněn při kontrole Kybernetických požadavků využít třetí stranu. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám, včetně odpovědnosti za způsobenou újmu.
- 20.6. Dodavatel umožní Objednateli kontrolu Kybernetických požadavků provedenou prostředky Objednatele nebo třetí strany, a to v lokalitě Dodavatele i vzdáleně, pokud to technické prostředky Dodavatele umožňují.
- 20.7. Dodavatel se zavazuje poskytnout Objednateli součinnost minimálně v rozsahu deset (10) ČD při provádění každého zákaznického auditu ze strany Objednatele a pro tuto činnost zajistit účast kvalifikovaných pracovníků.
- 20.8. Dále se Dodavatel zavazuje zjištěné nedostatky:
- 20.8.1. na základě provedení hodnocení rizik dle čl. 3 **Přílohy č. 9** této Smlouvy; nebo
 - 20.8.2. v rámci zákaznického auditu dle odst. 20.7 této Smlouvy;
- odstranit ve lhůtě určené v písemném oznámení Objednatele. Nestanoví-li Objednatel lhůtu v písemném oznámení, zavazují se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevyší devadesát (90) dnů.
- 20.9. Odstavce 20.4 až 20.7 této Smlouvy se neaplikují, pokud je Dodavatel pro poskytování předmětu plnění orgánem nebo osobou uvedenou v § 3 písm. a) až g) ZKB, přičemž se Objednatel zavazuje jej informovat, pokud jej bude považovat za provozovatele ve smyslu § 3 písm. c) až f) ZKB.
- 20.10. Dodavatel se dále dle této Smlouvy zavazuje:
- 20.10.1. poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků;
 - 20.10.2. na základě výzvy Objednatele bez zbytečného odkladu předat bezpečným způsobem a ve strojově čitelné podobě ve formátu uvedeném ve výzvě Objednatele jakákoli data předaná mu Objednatelem nebo získaná či vytvořená jiným způsobem při plnění Smlouvy v dispoziční sféře Dodavatele;
 - 20.10.3. odstranit veškerá data dle předchozího odstavce při ukončení účinnosti Smlouvy nebo na základě písemné žádosti Objednatele, a to nejpozději do čtrnácti (14) dní a za dozoru zástupce Objednatele, přičemž v případě, že Dodavatel bude mít na svých nosičích data vysoké či kritické úrovně důležitosti určené v souladu s přílohou č. 1 VKB, má povinnost tyto nosiče fyzicky protokolárně zlikvidovat, případně je předat k likvidaci Objednateli;

- 20.10.4. na požádání s Objednatelem konzultovat kdykoli v průběhu poskytování Plnění dle této Smlouvy detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků;
- 20.10.5. neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků, které nastanou kdykoli v průběhu trvání této Smlouvy;
- 20.10.6. informovat Objednatele o významné změně ovládání Dodavatele. Ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), či ekvivalentní postavení dle VKB;
- 20.10.7. bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní;
- 20.10.8. bezodkladně informovat Objednatele o bezpečnostních incidentech, které mohou ovlivnit poskytování Plnění dle této Smlouvy; a
- 20.10.9. při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům a jejichž následkem může vzniknout újma nebo nesoulad se ZKB a VKB nebo jinými obecně závaznými právními předpisy.

21. ŘEŠENÍ SPORŮ

- 21.1. Práva a povinnosti Smluvních stran touto Smlouvou výslovně neupravené se řídí OZ a příslušnými právními předpisy souvisejícími.
- 21.2. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou, včetně sporů o její výklad či platnost a usilovat se o jejich vyřešení nejprve smírně prostřednictvím jednání oprávněných osob nebo pověřených zástupců, a to do šedesáti (60) dnů ode dne doručení výzvy ke smírnému vyřešení sporu zaslané kteroukoliv Smluvní stranou druhé Smluvní straně.
- 21.3. Nebude-li sporná záležitost vyřešena dle odst. 21.2 této Smlouvy do šedesáti (60) dnů ode dne doručení výzvy ke smírnému vyřešení sporu zaslané kteroukoliv Smluvní stranou druhé Smluvní straně, bude tento spor rozhodován s konečnou platností u příslušného obecného soudu České republiky. Smluvní strany se dohodly, že místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.

22. ZÁVĚREČNÁ USTANOVENÍ

- 22.1. Tato Smlouva představuje úplnou dohodu Smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných osobami oprávněnými jednat jménem Smluvních stran, přičemž jakákoliv změna Smlouvy bude provedena v souladu se ZZVZ.
- 22.2. Pokud by se kterékoliv ustanovení této Smlouvy ukázalo být neplatným nebo nevynutitelným nebo se jím stalo po uzavření této Smlouvy, pak tato skutečnost nepůsobí neplatnost ani nevynutitelnost ostatních ustanovení této Smlouvy, nevyplyvá-li z donucujících ustanovení právních předpisů jinak. Smluvní strany se zavazují takové neplatné či nevynutitelné ustanovení nahradit v souladu se ZZVZ platným a vynutitelným ustanovením, které je svým obsahem nejbližší účelu neplatného či nevynutitelného ustanovení.
- 22.3. Smluvní strany souhlasí s uveřejněním plného znění této Smlouvy v registru smluv podle ZRS a rovněž na profilu Objednatele, případně i na dalších místech, kde tak stanoví právní předpis. Uveřejnění Smlouvy prostřednictvím registru smluv zajistí Objednatel.
- 22.4. Právní vztahy v této Smlouvě neupravené nebo upravené jen částečně se řídí právním řádem České republiky, zejména příslušnými ustanoveními OZ.
- 22.5. Veškerá práva a povinnosti vyplývající z této Smlouvy přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce Smluvních stran.
- 22.6. Dodavatel není oprávněn postoupit peněžité nároky vůči Objednateli na třetí osobu bez předchozího písemného souhlasu Objednatele.
- 22.7. Nedílnou součástí Smlouvy tvoří tyto přílohy:

Příloha č. 1:	Technická specifikace
Příloha č. 2:	Specifikace Podpory výrobce
Příloha č. 3:	Specifikace Provozní podpory
Příloha č. 4:	Harmonogram
Příloha č. 5:	Specifikace ceny Plnění
Příloha č. 6:	Oprávněné osoby, realizační tým a seznam poddodavatelů
Příloha č. 7:	Seznam ICT standardů
Příloha č. 8:	Ujednání o ochraně a zpracování osobních údajů
Příloha č. 9:	Požadavky na zajištění kybernetické bezpečnosti (Kybernetické požadavky)

Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Objednatel

V Praze dne dle data el. podpisu

.....
Hlavní město Praha

Mgr. Jiří Károly

ředitel odboru informatických činností

HMP

Dodavatel

V Praze dne dle data el. podpisu

**Tomáš
Příbyl**

Digitálně podepsal
Tomáš Příbyl
Datum: 2022.10.13
10:23:24 +02'00'

.....
Corpus Solutions a.s.

Ing. Tomáš Příbyl

předseda představenstva

Příloha č. 1 – Technická specifikace hardware

	Typ zařízení	SKU (Stock Keeping Unit)	Počet
A	6600 Plus appliance with SandBlast subscription package for 1 year	CPAP-SG6600-PLUS-SNBT	4
	Next Generation Threat Prevention for additional 2 years for 6600 PLUS Appliance	CPSB-NGTP-6600-PLUS-2Y	4
	Collaborative Premium for 3Y (36 měsíců)	CPCES-CO-PREMIUM-ADD	1
B	6700 Plus appliance with SandBlast subscription package for 1 year	CPAP-SG6700-PLUS-SNBT	2
	Next Generation Threat Prevention for additional 2 years for 6700 PLUS Appliance	CPSB-NGTP-6700-PLUS-2Y	2
	Collaborative Premium for 3Y (36 měsíců)	CPCES-CO-PREMIUM-ADD	1
C	7000 Plus appliance with SandBlast subscription package for 1 year	CPAP-SG7000-PLUS-SNBT	2
	Next Generation Threat Prevention for additional 2 years for 7000 PLUS Appliance	CPSB-NGTP-7000-PLUS-2Y	2
	Collaborative Premium for 3Y (36 měsíců)	CPCES-CO-PREMIUM-ADD	1

Příloha č. 2 – Specifikace Podpory výrobce

Příloha č.2.1-CES-datasheet-collaborative-enterprise-support

Příloha č.2.2-collaborative-enterprise-support-sla

Přílohy jsou připojeny v závěru této Smlouvy

Příloha č. 3 – Specifikace Provozní podpory

V případech, kdy Dodavatel v rámci poskytování Služeb (Service level Agreement, SLA), jejichž předmět je smluvně vymezen příslušným Katalogovým listem, nedosáhne stanovené (dohodnuté) úrovně plnění během vyhodnocovacího období, vzniká tímto Objednateli nárok na jednorázovou slevu z ceny za Služby pro dané vyhodnocovací období. Za nedosažení stanovené (dohodnuté) úrovně plnění se nepočítá doba plánované odstávky dané Služby. Výše jednorázové slevy bude stanovena dle příslušného SLA parametru, který byl porušen, a dle úrovně porušení (specifikovaná jednotlivě pro každý SLA parametr).

V případě, že dojde k nedodržení více dílčích SLA parametrů v rámci jedné Služby, platí, že sleva z ceny se uplatní ke všem nedodržným dílčím SLA parametrům.

Dostupnost

Dostupností je míněna dostupnost Služby v průběhu zaručené provozní doby, vyhodnocovaná v rámci vyhodnocovacího období. Na dostupnost, resp. nedostupnost Služby mají dopad incidenty kategorie A (incidenty kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují). Dostupnost Služby je vyhodnocována v procentech za vyhodnocovací období.

Provozní doba zaručená

Provozní dobou zaručenou je míněna provozní doba Služby, v průběhu, které je Objednatel požadovaná a současně Dodavatelem garantovaná plná nebo omezená dostupnost Služby, a to včetně podpory ze strany Dodavatele. Provozní doba zaručená je měřena/vyhodnocována v jednotkách času (v hodinách). Dostupnost Služby, resp. úroveň/rozsah její dostupnosti v době mimo zaručenou provozní dobu je specifikována příslušným katalogovým listě.

Maximální doba výpadku

Maximální dobou výpadku je míněno maximální časové období, po které je v rámci zaručené provozní doby přípustná jednorázová nedostupnost Služby. Maximální doba výpadku je vyhodnocována v jednotkách času (v hodinách).

Maximální doba nedostupnosti dat

Maximální dobou nedostupnosti dat je míněna ztráta nebo nedostupnost transakčních, aplikačních či systémových dat využívaných/spravovaných danou Službou, vyhodnocovaná v rámci vyhodnocovacího období. Maximální doba nedostupnosti dat je vyhodnocována v jednotkách času (v hodinách).

Maximální doba servisní odezvy

Reakční dobou servisní odezvy je míněna doba, do které je Dodavatel povinen zareagovat na nový záznam v helpdeskovém systému, který byl založen v rámci zaručené provozní doby. Maximální doba servisní odezvy je vyhodnocována v jednotkách času (v minutách).

Odstranění výpadku – A, B, C

Jednotlivé kategorie incidentů jsou uvedeny v příslušných katalogových listech. Odstranění výpadku je měřeno/vyhodnocováno v jednotkách času (v hodinách pro kategorii A, ve dnech pro kategorie B a C).

Čas potřebný k odstranění hardwarové závady třetí smluvní stranou (např. servis třetích stran, jakožto přímým smluvním partnerem Objednatele), se do doby vyřešení výpadku nezapočítává.

Plánované odstávky dané Služby se do doby výpadku nezapočítávají.

Katalogový list	KL01 – Obecné pravidelné služby a SLA		
Název služby	Provoz a správa – pravidelné služby a SLA		
VYMEZENÍ SLUŽBY			
Prostředí	Produkční		
ROZSAH POŽADOVANÝCH ČINNOSTÍ			
1. Provoz služeb - Technická podpora je garantovaná dostupností 24x7x365 na telefonní lince uvedené ve smlouvě. - Kontrola logů, hlášení o možných chybách v provozovaných systémech (na týdenní bázi). - Kontrola monitoringu služby (na měsíční bázi). - Návrh preventivních opatření vyplývajících z monitoringu a profylaktických činností s cílem předejít možným výpadkům a omezením služby. - Odborná technická podpora a odstraňování závad (na denní bázi). 2. Správa služeb - Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobce (na týdenní bázi). - Údržba a zajištění dostupnosti služeb. - Analýza vhodnosti a potřebnosti implementace opravného balíku. - Návrh opatření a postupu implementace opravného balíku ke schválení Objednateli. - Implementace schválených požadavků na změnu konfigurace služby. 3. Součinnost a konzultace v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře (I společně s dodavateli technologií). 4. Správa a aktualizace provozní dokumentace v rozsahu: - postupy pro provoz a správu služby, - postupy pro obnovu služby ze záloh jednotlivých systémů. 5. Správa a aktualizace technické dokumentace v rozsahu: - aktuální přehled infrastruktur jednotlivých systémů/aplikací služby, - aktuální přehled parametrů jednotlivých aplikací, - správa konfigurací předmětných služeb. 6. Reporting - Objednatel obdrží servisní report na měsíční bázi. - Pravidelný zpráva za plnění servisní služby za 3 měsíce v sídle Objednatele, sestávající se z přípravy a prezentace výstupů z provedených prací za minulé 3 kalendářní měsíce, včetně výstupů ze systémů Monitoring a HelpDesk. Report, který bude prezentován ze strany projektového manažera, bude obsahovat výkaz veškerých incidentů, požadavků a činností provedených v rámci smlouvy, včetně detailním náhledu výkazu práce za každých odpracovaných 0,5 hod.			
SERVICE LEVEL AGREEMENT (SLA)			
Vyhodnocovací období	1 kalendářní měsíc		
SLA parametry	Jednotka	Hodnota	
Dostupnost	[%/měs]	98	
Provozní doba zaručená	[hod-hod]	24x7x365	
Upřesnění kategorií incidentů a závad			

Kategorie A	Nedostupnost některé z klíčových technických součástí
Kategorie B	Závažná nebo výpadek části služby, které způsobí sníženou dostupnost služby, avšak nezpůsobí celkovou nedostupnost služby.
Kategorie C	Ostatní závady nespádající do kategorie A nebo B
Způsob kontroly	
Do dostupnosti jsou počítány pouze incidenty typu A, incidenty a výpadky kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují. Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřicí body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Pravidelný zpráva o plnění servisní služby bude poskytnuta 1x měsíčně písemnou formou.	
PODMÍNKY A OMEZENÍ SLUŽBY	
Další podmínky či omezení	Dodavatel je povinen poskytnout součinnost při zajištění technické podpory s výměnou HW/komponent s ukončením opravy do následujícího pracovního dne. Zajištění administrace technologie, zahrnující správu a profylaxi všech zařízení HW technologie, včetně instalace nových verzí a opravných patchů, kontrolu logů, výkonnostních parametrů, bezpečnostní update a případně provedení úprav nebo optimalizace nastavení bude probíhat formou vzdáleného přístupu.

Katalogový list	KL02 – Monitoring a dohledové služby
Název služby	Monitoring zařízení
VYMEZENÍ SLUŽBY	
Prostředí	Produkční
ROZSAH POŽADOVANÝCH ČINNOSTÍ	
Provoz služby - Udržování aktuálnosti všech zařízení a sítí pokrytých službou KL04-12 provozovaných služeb v prostředí dohledového nástroje. - Udržování aktuálnosti všech závislostí mezi sledovanými zařízeními. - Definice a nastavování limitů u jednotlivých triggerů. - Udržování aktuálnosti nastavení SLA sledovaných zařízení pro automatickým zakládání ticketu typu Incident v ticketovacím systému HelpDesk. - Kontrola logů sledovaných zařízení (na denní bázi). - Kontrola výkonnosti a performance monitoring sledovaných technologií (na týdenní bázi). - Incident management – Odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support (na týdenní bázi). - Problem management – Návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře (minimálně kvartálně nebo dle aktuální situace). - Reporting z prostředí dohledového nástroje a helpdesku.	
Popis dohledového systému	
- Monitoring poskytuje oběma smluvním stranám včasné varování, formou e-mailové, SMS notifikace nebo hlasové zprávy, o výpadcích, trendech a historii chodu důležitých technologií IT infrastruktury a v omezeném rozsahu aplikačních systémů monitorovaných po dohodě s Objednatelém. - Monitoring ICT infrastruktury dostupný v režimu 24x7x365. Dodavatel zajistí plnění záznamů o prvcích a zařízeních v rámci dohledového nástroje, za využití týmu specialistů, kteří neustále vyhodnocují a zpracovávají hlášení událostí dohledovým systémem. - Dodavatel je povinen přistupovat přes zabezpečený protokol HTTPS. - Monitoring sleduje fyzické i virtuální prvky a technologie. - Součástí předmětu plnění musí být i reporting z dohledového nástroje, který musí umožňovat ad hoc nebo individuální grafické reporty z nasbíraných hodnot. Je možné definovat vlastní skupiny pro sledování plnění SLA nad jednotlivými technologiemi.	
Způsob kontroly	
Pravidelná zpráva o plnění servisní služby bude poskytnuta 1x měsíčně písemnou formou.	
PODMÍNKY A OMEZENÍ SLUŽBY	
Další podmínky či omezení	n/a

Katalogový list		KL03 – HelpDesk služby	
Název služby		HelpDesk služby	
VYMEZENÍ SLUŽBY			
Prostředí		Produkční	
ROZSAH POŽADOVANÝCH ČINNOSTÍ			
HelpDesk služby a. Dostupnost služby HelpDesku v režimu 24x7x365. b. Poskytovaná služba v souladu s ITIL. c. Minimální počet pracovníků HelpDesku (v režimu 24x7x365) jsou 3 pracovníci – Operátor SD, L1 support výjezdový technik a L2 senior systém administrátor. d. Technické vybavení a prostory splňují bezpečnostní požadavky a požadavky normy ISO27001. e. Zajištění a evidence všech požadavků a servisních zásahů – telefonních, emailových, monitoring notifikací – ServiceDesk@corpus.cz; +420 241 020 701; https://jira.corpus.cz f. Vyhodnocení požadavků a událostí (dopad, priorita, prvotní analýza). g. Dispečink a dohled nad řešením otevřených požadavků, událostmi a logistikou techniků, servisních zásahů.			
HelpDesk nástroj a. HelpDeskový nástroj musí být zabezpečen protokolem HTTPS. b. Zajišťuje automatické potvrzení o přijetí požadavku. c. Je nastaven pro příjem automatizovaných notifikací o incidentech z monitorovacího nástroje. d. Reporting – zajištění individuálních reportů z databáze požadavků a událostí.			
Znůsob kontrol			
Pravidelná zpráva o plnění servisní služby bude poskytnuta 1x měsíčně písemnou formou.			
SERVICE LEVEL AGREEMENT (SLA)			
Vyhodnocovací období		1 kalendářní měsíc	
SLA parametry		Jednotka	Hodnota
Dostupnost		hod	24x7x365
Provozní doba zaručená		[hod-hod1]	00:00 – 23:59
Max. doba servisní odezvy		[hod]	2
PODMÍNKY A OMEZENÍ SLUŽBY			
Další podmínky či omezení		Způsoby hlášení jsou: a. e-mailem – helpdesk@corpus.cz b. telefonicky – +420 241 020 701	

Katalogový list	KL04 – Provoz a správa firewallů interního perimetru	
Název služby	Provoz a správa - interní firewall	
VYMEZENÍ SLUŽBY		
Prostředí	Produkční	
ROZSAH POŽADOVANÝCH ČINNOSTÍ		
1. Provoz technologie a. Kontrola výkonnosti a performance monitoring (na vyžádání). b. Návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře (dle aktuální situace). c. Odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support (na denní bázi). d. Provádění pravidelných záloh SW konfigurací (aktualizace záloh po každé změně). Zálohování bude prováděno na centrální úložiště Zadavatele. 2. Správa aktivních prvků a. Konfigurace a správa. b. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobců. c. Analýza vhodnosti a potřeby implementace opravného balíku. d. Návrh opatření a postupu implementace opravného balíku ke schválení Zadavatelí. e. Implementace schválených požadavků na změnu konfigurace aktivních prvků. f. Předkládání návrhů na optimalizaci. 3. Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře (společně s dodavateli technologií). Účast na jednání provozních a pracovních týmů Zadavatele. 4. Správa a aktualizace provozní dokumentace v rozsahu: a. postupy pro provoz a správu každého typu zařízení, b. postupy pro obnovu zařízení ze záloh. 5. Správa a aktualizace technické dokumentace v rozsahu: a. aktuální schéma fyzického zapojení, b. aktuální schéma logického zapojení, c. aktuální přehled verzí OS aktivních prvků, d. reporting. 6. Další expertní zásahy do technologie a. Výkonnostní optimalizace bezpečnostních politik. b. Řízené pravidelné aktualizace pokročilých bezpečnostních funkcionalit. c. Kontrola detekce a záchytů útoků z interních sítí		
SERVICE LEVEL AGREEMENT (SLA)		
Vyhodnocovací období	1 kalendářní měsíc	
SLA parametry	Jednotka	Hodnota
Dostupnost	[%/měs]	99
Provozní doba zaručená	[hod-hod]	0-24 (7x24)
Max. doba výpadku	[hod]	8
Max. doba nedostupnosti dat	[hod]	8
Max. doba servisní odezvy	[min]	120
Odstranění výpadku – A	[hod]	8

Odstranění výpadku – B	[dny]	3
Odstranění výpadku – C	[dny]	5
Upřesnění kategorií incidentů a závad		
Kategorie A	Závada: a. způsobí celkovou nedostupnost (nefunkčnost) funkčního celku; b. je způsoben hardwarovou poruchou zařízení funkčního celku znemožňující provozuschopnost tohoto zařízení alespoň s omezeným výkonem. Neplatí pro zařízení, které je provozováno v režimu vysoké dostupnosti a jehož funkci zajišťuje automaticky náhradní řešení (redundance, high availability, cluster) se stejným nebo sníženým výkonem; c. je způsoben softwarovou poruchou v rámci funkčního celku, znemožňující jeho provozuschopnost alespoň s omezeným výkonem; d. vznikne jako důsledek jiných neplánovaných výpadků (elektrické energie) a vyžaduje provedení kontrolovaného obnovení provozuschopnosti funkčních celků; e. znemožňuje uživatelům provádět standardní pracovní činnosti alespoň náhradním způsobem; f. je způsoben bezprostředním ohrožením IT bezpečnosti zákazníka a kompromitace ICT systémů včetně pracovních stanic (globální virová infekce, apod.).	
Kategorie B	Závada: a. způsobí snížení výkonnosti funkčních celků; b. je způsoben hardwarovou poruchou zařízení funkčního celku, která umožňuje provozuschopnost tohoto zařízení s omezeným výkonem; c. je způsoben softwarovou poruchou v rámci funkčního celku, která umožňuje provozuschopnost instalovaného software s omezeným výkonem;	
Kategorie C	Závada: a. nemá vliv na dostupnost funkčních celků; b. nemá vliv na výkonnost funkčních celků; c. může však ovlivňovat pracovní procesy Zákazníka.	
Způsob kontroly		
Do dostupnosti jsou počítány pouze incidenty typu A, incidenty a výpadky kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují. Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřicí body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Pravidelná zpráva o plnění servisní služby bude poskytnuta 1x měsíčně písemnou formou.		
PODMÍNKY A OMEZENÍ SLUŽBY		
Limit objemu služby	Počet spravovaných zařízení 8.	
Omezení	Součástí služby není placení roční podpory a maintenance poplatků výrobcům software a hardware. Součástí služby nejsou migrace či instalace nových verzí systémů.	
Další podmínky či omezení	n/a	

Příloha č. 4 – Harmonogram

Zadavatel požaduje, aby Dodavatel dodržel následující harmonogram.

D = den účinnosti Smlouvy

U = den ukončení Smlouvy

Krok	Zahájení	Ukončení	Popis činností
1	D	D+ 5 pracovních dní =D ₁	Vytvoření Implementačního plánu
2	D ₁	D ₁ + 3 pracovní dny=D ₂	Připomínkové řízení a akceptace Implementačního plánu, zapracování všech připomínek Objednatele
3	D	Nejpozději do 60 dnů ode dne akceptace Implementačního plánu = D ₃	Dodávka hardware
4	D ₃	D ₃ + 30 pracovních dní = D ₄	Implementace dle schváleného Implementačního plánu
5	D ₃	D ₃ +36 měsíců=U	Poskytování Podpory výrobce
6	D ₃	D ₃ +36 měsíců=U	Poskytování Provozní podpory

Příloha č. 5 – Specifikace ceny Plnění

Příloha č. 6 – "Tabulka pro zpracování nabídkové ceny" zadávací dokumentace					
Cena za HW/software (HW) a Software (SW) upgrade stávajícího řešení včetně podpory	Typ zařízení	SKU (Stock Keeping Unit)	Požadovaný počet jednotek	Cena za jednotku v Kč bez DPH	Cena celkem v Kč bez DPH (tj. za počet jednotek)
A	6600 Plus appliance with SandBlast subscription package for 1 year	CPAP-SG6600-PLUS-SNET	4	1 550 784,00 Kč	6 203 136,00 Kč
	Next Generation Threat Prevention for additional 2 years for 6600 PLUS Appliance	CPSB-NGTP-6600-PLUS-2Y			
	Collaborative Premium (36 měsíců)	CPCES-CO-PREMIUM-ADD			
B	6700 Plus appliance with SandBlast subscription package for 1 year	CPAP-SG6700-PLUS-SNET	2	2 198 124,00 Kč	4 396 248,00 Kč
	Next Generation Threat Prevention for additional 2 years for 6700 PLUS Appliance	CPSB-NGTP-6700-PLUS-2Y			
	Collaborative Premium (36 měsíců)	CPCES-CO-PREMIUM-ADD			
C	7000 Plus appliance with SandBlast subscription package for 1 year	CPAP-SG7000-PLUS-SNET	2	3 280 170,00 Kč	6 560 340,00 Kč
	Next Generation Threat Prevention for additional 2 years for 7000 PLUS Appliance	CPSB-NGTP-7000-PLUS-2Y			
	Collaborative Premium (36 měsíců)	CPCES-CO-PREMIUM-ADD			
Cena za plnění "A,B a C" celkem v Kč bez DPH					17 159 724,00 Kč
Cena za implementační plán a implementaci			Přepokládaný počet ČD (pozn. Počet ČD je stanoven pouze pro účely hodnocení nabídek, skutečný počet ČD může být odlišný podle potřeb Závazitele. Dodavatel není oprávněn si nárokovat uvedený počet ČD)	Cena za 1 ČD v Kč bez DPH	Cena celkem v Kč bez DPH (tj. za počet jednotek)
			40	10 000,00 Kč	400 000,00 Kč
Cena provozní podpory za jeden měsíc			Požadovaný počet měsíců	Cena za 1 měsíc v Kč bez DPH	Cena celkem v Kč bez DPH (tj. za počet jednotek)
			36	50 000,00 Kč	1 800 000,00 Kč
Celková nabídková cena (v Kč bez DPH)					19 359 724,00 Kč

Legenda:

„ČD“ = Běžikodem ve zsumární čas odpovídající práci jednotlivých členů realizačního týmu za dobu jednoho pracovního dne, tj. 8 hodin u Objedvatele, včetně všech případných souvisejících nákladů na dopravu, stravování, ubytování apod.

Dodavatel vyplní pouze **žlutě podbarvené** buňky Tabulky pro zpracování nabídkové ceny. Ostatní buňky budou doplněny automaticky, dodavatel je však povinen překontrolovat správnost nastavených vzorů.

Závazitel souborně stanovuje, že celková nabídková cena dodavatelé nesmí být vyšší než 19 990 000,- Kč bez DPH. Dodavatel, který předloží nabídkovou cenu vyšší, bude ze zadávacího řízení vyloučen.

Příloha č. 6 – Oprávněné osoby, realizační tým a seznam poddodavatelů

Oprávněné osoby

Za Objednatele:

ve věcech smluvních:

Jméno a příjmení	Mgr. Jiří Károly
Adresa	Jungmannova 35/29, 11000 Praha 1
E-mail	
Telefon	

ve věcech obchodních:

Jméno a příjmení	Mgr. Jiří Károly
Adresa	Jungmannova 35/29, 11000 Praha 1
E-mail	
Telefon	

ve věcech technických:

Jméno a příjmení	Bc. Schneider Michael
Adresa	Jungmannova 35/29, 11000 Praha 1
E-mail	
Telefon	

Za Dodavatele:

ve věcech smluvních:

Jméno a příjmení	Mgr. Pavel Cvešpr
Adresa	Štětкова 1638/18, 140 00 Praha 4
E-mail	
Telefon	

ve věcech obchodních:

Jméno a příjmení	Mgr. Pavel Cvešpr
Adresa	Štětкова 1638/18, 140 00 Praha 4
E-mail	
Telefon	

ve věcech technických:

Jméno a příjmení	Lukáš Sosnovec
Adresa	Štětкова 1638/18, 140 00 Praha 4
E-mail	
Telefon	

Realizační tým Dodavatele

Pozice (role)	Identifikační a kontaktní údaje osoby	Dodavatel / člen společnosti dodavatelů / poddodavatel, k němuž osoba patří
Projektový manažer	Bc. Jakub Jeráček	Zaměstnanec dodavatele
Specialista Check Point č. 1	Ing. Lukáš Sosnovec	Zaměstnanec dodavatele
Specialista Check Point č. 2	Ing. Michal Gans	Zaměstnanec dodavatele
IT bezpečnostní analytik	David Bursík	Zaměstnanec dodavatele

Seznam poddodavatelů

1)

Název: [DOPLNÍ DODAVATEL]
Sídlo: [DOPLNÍ DODAVATEL]
Právní forma: [DOPLNÍ DODAVATEL]
Identifikační číslo: [DOPLNÍ DODAVATEL]
Rozsah plnění Smlouvy: [DOPLNÍ DODAVATEL – specifikace věcného plnění vč. procentuální rozsah]

2)

Název: [DOPLNÍ DODAVATEL]
Sídlo: [DOPLNÍ DODAVATEL]
Právní forma: [DOPLNÍ DODAVATEL]
Identifikační číslo: [DOPLNÍ DODAVATEL]
Rozsah plnění Smlouvy: [DOPLNÍ DODAVATEL – specifikace věcného plnění vč. procentuální rozsah]

atd. [DOPLNÍ DODAVATEL]

Příloha č. 7 – Seznam ICT standardů

Objednatel v souladu s odst. 10.3.13 Smlouvy Dodavateli předal následující ICT standardy:

ID	Název standardu
1	SA01 Správa koncových zařízení
2	SB04 Služby datového centra – virtualizace
3	SB05 Pronájem optických vláken a DWDM
4	SB06 Správa Firewall
5	SB07 Správa LAN
6	SB08 SLA Container
7	SB09 Antivir
8	SB10 Správa WAN
9	SB11 Poskytování diskového prostoru
10	SB12 Poskytování výpočetního výkonu (HW)
11	SB13 Identity and access management (IAM)
12	SB14 Správa e-mailových služeb
13	SB15 Internet access
14	SB16 VPN gateway
15	SB17 Poskytování služby ServiceDesk
16	SB18 Poskytování monitoringu infrastruktury a služeb
17	SB19 Poskytování služby Licence management
18	SB20 DNS, DHCP a AD
19	SB21 Správa certifikátu a CA
20	SC01 Generická aplikace
21	MC01 Provoz programového vybavení Celopražského významu
22	MC02 Poskytnutí datového prostoru
23	MC03 Bezpečné úložiště
24	MC04 Poskytování výpočetního výkonu v datovém centru
25	MC05 Poskytování podpůrného programového vybavení

Příloha č. 8 – Ujednání o ochraně a zpracování osobních údajů

S ohledem na předmět této Smlouvy smluvní strany předpokládají, že Dodavatel bude zpracovávat osobní údaje subjektů údajů ve smyslu Nařízení GDPR při poskytování některého Plnění dle této Smlouvy, tj. zejména osob evidovaných v informačních systémech Objednatele, ke kterým bude mít Dodavatel v rámci realizace Plnění přístup a dalších zaměstnanců a jiných osob Objednatele v souvislosti s realizací Plnění dle Smlouvy (dále jen „**Evidované osoby**“). Toto ujednání obsahuje rovněž ustanovení o zpracování osobních údajů dle Nařízení GDPR, mezi Objednatelem jako správcem osobních údajů a Dodavatelem jako zpracovatelem osobních údajů, uvedená níže.

1. OBECNÉ ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ EVIDOVANÝCH OSOB

- 1.1. Objednatel jako správce osobních údajů pověřuje Dodavatele jako zpracovatele osobních údajů zpracováváním osobních údajů v rozsahu nezbytném pro plnění Smlouvy a výhradně za účelem vyplývajícím z účelu Smlouvy.
- 1.2. Povinnosti Dodavatele týkající se ochrany osobních údajů se Dodavatel zavazuje plnit i po zániku účinnosti Smlouvy.
- 1.3. Dodavatel je povinen postupovat při zpracování osobních údajů v souladu s touto Smlouvou a Nařízením GDPR, a zpracovávat osobní údaje výlučně pro účel a v rozsahu, ve kterém mu byly předány a při zpracování postupovat jako odborník s řádnou péčí tak, aby neporušil žádné ustanovení Nařízení GDPR, či jiného právního předpisu nebo nezpůsobil skutečnost, která by znamenala porušení Nařízení GDPR, či jiného právního předpisu Objednatelem.
- 1.4. V případě ukončení této Smlouvy je Dodavatel povinen předat Objednateli protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li Dodavatel od Objednatele písemně jiné pokyny nebo nezavazují-li ho k dalšímu zpracování těchto osobních údajů explicitně vymezená plnění právních povinností. O těchto právních povinnostech je v případě ukončení této Smlouvy Dodavatel povinen Objednatele informovat.
- 1.5. Dodavatel je povinen dbát, aby žádná Evidovaná osoba neutrpěla újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu Evidovaných osob před neoprávněným zasahováním do soukromého a osobního života.
- 1.6. Dodavatel se zavazuje dodržovat všechny povinnosti, které mu jako zpracovateli osobních údajů vyplývají z Nařízení GDPR, jakož i z interních předpisů Objednatele a rozhodnutí či doporučení nebo stanovisek vydaných pro Objednatele příslušným

orgánem státní správy, s nimiž byl seznámen, a to včetně rozhodnutí či stanovisek nebo doporučení vydaných v budoucnu.

- 1.7. Za účelem plnění povinností v souvislosti s ochranou a zpracováním osobních údajů dle Smlouvy se Objednatel zavazuje bezodkladně po jejich obdržení poskytovat Dodavateli jakákoliv rozhodnutí či doporučení nebo stanoviska vydaná příslušným orgánem státní správy.
- 1.8. Dodavatel je povinen zajistit, že zpracovávání osobních údajů probíhá v souladu s Nařízením GDPR i v tom smyslu, že v případě, že je podle Nařízení GDPR či jiného příslušného právního předpisu vyžadováno jakékoli oznámení nebo jiný úkon vůči Úřadu pro ochranu osobních údajů či jinému správnímu orgánu, upozorní na tuto skutečnost Objednatele v dostatečném předstihu a v případě, že tím Objednatel Dodavatele pověří a zmocní, zajistí provedení těchto úkonů.
- 1.9. Pokud Dodavatel zjistí, že Objednatel porušuje povinnosti stanovené Nařízením GDPR, je povinen jej na to neprodleně upozornit.
- 1.10. V případě, kdy je ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu provedena kontrola zpracování osobních údajů Dodavatelem dle této Smlouvy či v případě zahájení správního řízení ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu ve vztahu k zpracování osobních údajů Dodavatelem dle této Smlouvy, je Dodavatel tuto skutečnost povinen okamžitě oznámit Objednateli a poskytnout mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového procesu, včetně kopií veškeré dokumentace (kontrolní protokol, zpráva o přijatých opatřeních k nápravě, atp.).
- 1.11. Dodavatel není oprávněn osobní údaje Evidovaných osob jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností dle této Smlouvy.
- 1.12. Dodavatel je dále povinen řádně vypořádávat požadavky a nároky vznesené subjekty údajů.
- 1.13. Dodavatel je povinen umožnit Objednateli na vyžádání kontrolu dodržování povinností dle této **Přílohy č. 8** Smlouvy, zejména přístupy do prostor, v nichž jsou osobní údaje uchovávány, předložení seznamu osob s přístupem k osobním údajům či doložení, že veškeré osoby přistupující k osobním údajům splňují požadavky pověřené osoby. Dodavatel je rovněž povinen umožnit Objednateli přístup do databáze s osobními údaji předáním přístupových údajů, a to vždy jednorázově na základě konkrétní žádosti Objednatele.

2. ROZSAH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

- 2.1. Dodavatel bude zpracovávat osobní údaje Evidovaných osob pouze v rozsahu nezbytném pro poskytování Plnění dle Smlouvy a pro výkon práv a povinností Dodavatele dle Smlouvy.
- 2.2. Zpracování osobních údajů Evidovaných osob je Dodavatel povinen provádět pouze v rozsahu nezbytně nutném pro plnění práv a povinností Dodavatele dle Smlouvy, přičemž se zejména bude jednat o následující kategorie osobních údajů:

2.2.1. Identifikační údaje;

2.2.2. Kontaktní údaje;

2.2.3. Údaje o plnění Smlouvy Evidovanými osobami.

3. ZÁRUKY O TECHNICKÉM A ORGANIZAČNÍM ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ EVIDOVANÝCH OSOB

- 3.1. Dodavatel je povinen zabezpečit v rozsahu Plnění poskytovaného dle této Smlouvy řádnou technickou a organizační ochranu zpracovávaných osobních údajů způsobem stanoveným v Nařízení GDPR či v jiných právních předpisech.
- 3.2. Dodavatel je povinen při zpracování osobních údajů zajistit ochranu osobních údajů minimálně na takové úrovni, aby byly dodrženy veškeré záruky o technickém a organizačním zabezpečení osobních údajů uvedené níže v této **Příloze č. 8** Smlouvy.
- 3.3. Dodavatel se zavazuje přijmout taková opatření, aby nemohlo dojít k neoprávněnému ani nahodilému přístupu k osobním údajům, k jejich úplné ani částečné změně, zničení či ztrátě, neoprávněným přenosům či sdružení s jinými osobními údaji, či k jinému neoprávněnému zpracování v rozporu se Smlouvou. Dodavatel zároveň užije taková opatření, která umožní určit a ověřit, komu byly osobní údaje předány. Tato povinnost platí i po ukončení zpracování osobních údajů.
- 3.4. Dodavatel se za účelem ochrany osobních údajů zavazuje zajistit zejména, že:
 - 3.4.1. Přístup k osobním údajům bude umožněn výlučně pověřeným osobám, které budou v pracovněprávním, příkazním či jiném obdobném poměru k Dodavateli, budou předem prokazatelně seznámeny s povahou osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se zpřístupněním osobních údajů a jejich zpracováním a dále budou prokazatelně poučeny o dalších povinnostech, které jsou povinny dodržovat tak, aby nedošlo k porušení Nařízení GDPR či jiných právních předpisů (dále jen „pověřené osoby“). Splnění těchto povinností zajistí Dodavatel

vhodným způsobem, zejména vydáním svých vnitřních předpisů, příp. prostřednictvím zvláštních smluvních ujednání. Dodavatel nesvěří zpracování osobních údajů jakékoliv třetí osobě bez předchozího písemného souhlasu Dodavatele a vždy vhodným způsobem zajistí, že jeho zaměstnanci a jiné osoby, které budou zpracovávat osobní údaje na základě Smlouvy s Dodavatelem, budou zpracovávat osobní údaje pouze za podmínek a v rozsahu Dodavatelem stanoveném a odpovídajícím této **Příloze č. 8** Smlouvy a za podmínek Nařízení GDPR, zejména zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací pověřených osob.

3.4.2. Při zpracování osobních údajů budou osobní údaje uchovávány výlučně na zabezpečených serverech nebo na zabezpečených nosičích dat a s využitím programového vybavení tak, aby byl vyloučen neoprávněný či nahodilý přístup k osobním údajům ze strany jiných osob, než pověřených zaměstnanců Dodavatele, jedná-li se o osobní údaje v elektronické podobě.

3.4.3. Při zpracování osobních údajů v jiné, než elektronické podobě budou osobní údaje uchovány v Objednatelem poskytnutých objektech a místnostech s náležitou úrovní zabezpečení, do kterých budou mít přístup výlučně pověřené osoby, a bude vedena řádná evidence o pohybu dokumentů obsahujících osobní údaje.

3.4.4. Přístup k osobním údajům bude pověřeným osobám umožněn výlučně pro účely zpracování osobních údajů v rozsahu a za účelem stanoveným touto Smlouvou. Přístup bude umožněn na základě přístupových kódů či hesel, tak aby byl každý přístup zaznamenán; osobní údaje budou pravidelně zálohovány.

3.5. Dodavatel se zavazuje na písemnou a odůvodněnou žádost Objednatele přijmout v přiměřené lhůtě další záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.

3.6. Dodavatel se zavazuje zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu s Nařízením GDPR a jinými právními předpisy, přičemž zajišťuje, kontroluje a odpovídá zejména za:

3.6.1. plnění pokynů pro zpracování osobních údajů specialisty Dodavatele, kteří mají bezprostřední přístup k osobním údajům,

- 3.6.2.zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování,
 - 3.6.3.zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a
 - 3.6.4.opatření, která umožní určit a ověřit, komu byly osobní údaje zpřístupněny nebo předány.
- 3.7. V případě zjištění porušení záruk dle této **Přílohy č. 8** Smlouvy je Dodavatel povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje, nejpozději však do tří (3) pracovních dnů poté, co je k tomu Objednatelem vyzván.
- 3.8. V oblasti automatizovaného zpracování osobních údajů je Dodavatel v rámci opatření podle předchozích odstavců povinen také:
- 3.8.1.zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze pověřené osoby,
 - 3.8.2.zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby,
 - 3.8.3.pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a zabránit neoprávněnému přístupu k datovým nosičům.

4. DOBA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A ODPOVĚDNOST DODAVATELE

- 4.1. Dodavatel bude osobní údaje Evidovaných osob zpracovávat podle této **Přílohy č. 8** Smlouvy po dobu poskytování Služeb dle Smlouvy.
- 4.2. Po uplynutí doby zpracování osobních údajů podle odstavce 4.1 této **Přílohy č. 8** Smlouvy mohou být osobní údaje Evidovaných osob Dodavatelem zpracovávány pouze v nezbytném rozsahu a výhradně pro plnění právních povinností, které na Dodavatele v souvislosti s ochranou osobních údajů dopadají, nebo za účelem ochrany práv a právem chráněných zájmů Objednatele a Dodavatele, nebo jiné dotčené osoby, a to nejdéle do konce pátého kalendářního roku následujícího po roce, v němž skončí doba zpracování osobních údajů podle této **Přílohy č. 8** Smlouvy. Dodavatel jednotlivé osobní údaje zlikviduje, jakmile pomine účel, pro který byly osobní údaje zpracovávány.

- 4.3. Dodavatel odpovídá subjektům údajů za škodu a nemajetkovou újmu způsobenou porušením povinnosti Dodavatele v souvislosti se zpracováním osobních údajů. Dodavatel dále odpovídá Objednateli za škodu a nemajetkovou újmu způsobenou vznikem povinnosti Objednatele hradit v souvislosti se zpracováním osobních údajů na základě Smlouvy nebo v souvislosti s ní jakoukoli náhradu škody a nemajetkové újmy subjektu osobních údajů nebo pokutu Úřadu pro ochranu osobních údajů či jinému správnímu orgánu v důsledku porušení povinností uložených Dodavateli zákonem nebo Smlouvou.
- 4.4. Dodavatel se zavazuje trvale vyhodnocovat plnění zákonných povinností souvisejících se zpracováním osobních údajů při provozu infrastruktury a průběžně navrhopat veškerá nezbytná opatření a změny ujednání o zpracování osobních údajů, které zajistí řádné plnění veškerých povinností Dodavatele souvisejících s ochranou osobních údajů.

Příloha č. 9 – Požadavky na zajištění kybernetické bezpečnosti

Za účelem povinností stanovených Objednateli jakožto povinné osobě VKB, je Dodavatel povinen nad rámec povinností stanovených Smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této **Přílohy č. 9** Smlouvy.

Dodavatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel právní úpravy bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je Objednatel oprávněn požadovat od Dodavatele přiměřenou součinnost i nad rámec povinností stanovených v této **Příloze č. 9** Smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti Dodavatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

1. Systém řízení bezpečnosti informací

1.1. Dodavatel se bude v rozsahu poskytování Plnění aktivně podílet na splnění povinností uvedených v § 3 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytování Plnění na své straně:

- 1.1.1. prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování Plnění dle Smlouvy;
- 1.1.2. na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaných Plnění dle Smlouvy, monitorovat je a vyhodnocovat jejich účinnost;
- 1.1.3. vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaných Plnění dle Smlouvy, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit;
- 1.1.4. stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování Plnění dle Smlouvy, přičemž bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby a práva a povinnosti ve vztahu k řízení bezpečnosti informací; a
- 1.1.5. stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

2. Řízení aktiv

- 2.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 4 VKB, které musí splnit Objednatel.
- 2.2. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění 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, HW prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli předložit do třiceti (30) dnů od nabytí účinnosti této Smlouvy a následně na vyžádání, a to po celou dobu trvání Smlouvy a do dvou (2) let po jejím ukončení.

3. Řízení rizik

- 3.1. Dodavatel se bude v rozsahu poskytování Plnění dle této Smlouvy aktivně podílet na splnění povinností uvedených v § 5 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytovaných Plnění na své straně:

3.1.1. řídit vlastní rizika, která mohou ovlivnit poskytování Plnění dle Smlouvy; a

3.1.2. v minimálním intervalu 1x ročně vytvořit a předložit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:

- a) vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;
- b) identifikaci a hodnocení rizik s vazbou na předmět plnění;
- c) realizovaná bezpečnostní opatření;
- d) nepokrytá bezpečnostní rizika a návrh opatření;
- e) vyhodnocení bezpečnostních událostí a incidentů; a
- f) aktuální stav souladu Dodavatele s těmito Kybernetickými požadavky.

4. Organizační bezpečnost

- 1.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 6 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu předmětu plnění na své straně:

4.1.1. Jmenovat nejpozději do pěti (5) dnů po uzavření této Smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi smluvními

stranami (dále také jen „**Kontaktní osoba**“). Kontaktní osobu sdělí Dodavatel písemně Objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně Dodavatele nemá dopad na ustanovení článku 13 Smlouvy týkající se odpovědných osob ve věcech smluvních a technických.

4.1.2. Využívat pro poskytování Plnění pouze oprávněných osob, které byly řádně seznámeny příslušnými ustanoveními interních řídicích aktů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování Plnění.

5. Řízení dodavatelů

5.1. Dodavatel se bude v rozsahu poskytovaných Plnění dle této Smlouvy aktivně podílet na splnění povinností uvedených v § 8 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytovaných Plnění na své straně:

5.1.1. využívá-li při poskytování Plnění poddodavatele, zajistit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Dodavatel zavazuje doložit Objednateli do deseti (10) dnů od účinnosti Smlouvy na jejímž plnění se budou poddodavatelé podílet, písemným prohlášením o dodržování Kybernetických požadavků u svých poddodavatelů; a

5.1.2. pokud při poskytování Plnění dochází ke zpracování osobních údajů, zajistit nad rámec čl. 14 Smlouvy a **Přílohy č. 9** Smlouvy uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této Smlouvy) ve smyslu příslušných ustanovení Nařízení.

6. Bezpečnost lidských zdrojů

6.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 9 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytovaných Plnění na své straně:

6.1.1. zajistit, aby Kontaktní osoba nejpozději do třiceti (30) dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování Plnění za stranu Dodavatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních řídicích aktů Objednatele;

6.1.2. dodržovat příslušná ustanovení interních řídicích aktů Objednatele v rozsahu, v jakém byl s těmito akty seznámen, přičemž

prokazatelným seznámením je školení pracovníků Dodavatele zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení;

6.1.3.v případě, že je součástí Plnění služba dohledu nad plněním, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění; a

6.1.4.zajistit, aby osoby podílející se na poskytování Plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:

- a) pro uložení a sdílení dat a informací Objednatele využívaly pouze k tomu schválené prostředky (aktiva);
- b) neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
- c) Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo Autorským zákonem;
- d) nenavštěvovaly internetové stránky s eticky nevhodným obsahem;
- e) nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;
- f) 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; a
- g) nepodílely se s prostředky Objednatele na šíření spamu ani škodlivého softwaru.

6.2. Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele zpracování osobních údajů pracovníků Dodavatele, kteří se podílejí na zajištění Plnění. Pokud nebude Objednateli umožněno osobní údaje dotčených pracovníků Dodavatele v rámci plnění Smlouvy zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.

7. Řízení provozu a komunikací

7.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 10 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytování Plnění na své straně:

- 7.1.1. zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování Plnění;
- 7.1.2. na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře; a
- 7.1.3. zajistit, že pro poskytování Plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a Autorský zákon.

8. Řízení změn

- 8.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 11 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytování Plnění na své straně:

- 8.1.1. přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny; a
- 8.1.2. aktivně spolupracovat při testování významné změny.

9. Řízení přístupu

- 9.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 12 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytování Plnění na své straně:

- 9.1.1. přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele;
- 9.1.2. zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Dodavatele, pokud sdílený přístup nevyžaduje využívaná technologie, přičemž v takovém případě musí Dodavatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání účinnosti této Smlouvy a dva (2) roky po ukončení její platnosti;
- 9.1.3. 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 / 1 den);

- 9.1.4. zajistit, aby osoby podílející se na poskytování Plnění a mající přístup k informačním aktivům Objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám;
a
- 9.1.5. průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Dodavatele, které přistupují do prostředí Objednatele.

9.2. Dodavatel bere na vědomí, že:

- 9.2.1. přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Dodavatele / poddodavatele Dodavatele, a to na základě požadavku Dodavatele na přístup;
- 9.2.2. přidělení oprávnění zaměstnanci Dodavatele musí být řízeno principem nezbytného minima a není nárokové; a
- 9.2.3. v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Dodavatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Objednatele).

10. Akvizice, vývoj a údržba

- 10.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 13 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytování Plnění na své straně:

10.1.1. zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění; a

10.1.2. předat Objednateli dokumentaci minimálně v následujícím rozsahu:

- a) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
- b) dokumentaci obsahující popis autorizačního konceptu a oprávnění; a
- c) dokumentaci obsahující instalační a konfigurační postupy.

- 10.2. V případě, že poskytované Služby dle Smlouvy zahrnují vývoj softwaru, zavazuje se Dodavatel:

10.2.1. dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu;

- 10.2.2. na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit Objednateli vyvíjený kód SW a výstupy z provedeného codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), po jeho dokončení, pokud není v této Smlouvě stanoveno jinak, a to zejména za účelem ověření skutečnosti, zda Dodavatel postupuje či postupoval při poskytování plnění v souladu se Smlouvou a těmito Kybernetickými požadavky;
- 10.2.3. poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání;
- 10.2.4. zajistit, že Služby budou obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve Smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.);
- 10.2.5. pokud je součástí Plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Objednatele;
- 10.2.6. zajistit bezpečnost testovacího prostředí u Dodavatele a ochranu poskytnutých testovacích dat Objednatelem;
- 10.2.7. zajistit, že do produkčního prostředí Objednatele bude dodán jen předmětem Smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování Plnění;
- 10.2.8. zajistit, že v rámci poskytovaných Plnění bude dodáváný software:
- a) v souladu s bezpečnostními politikami a standardy Objednatele;
 - b) otestován na soulad s bezpečnostními politikami Objednatele (platí pro Dodavatele, pokud byl s takovými bezpečnostními politikami seznámen);
- 10.2.9. instalovat software pouze na základě Objednatelem předem schválených migračních postupů; a
- 10.2.10. nevyvíjet, nekompilovat a nešířit v prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení

dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

11. Zvládání kybernetických bezpečnostních událostí a incidentů

11.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 14 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytování Plnění na své straně:

- 11.1.1. stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů;
- 11.1.2. bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby;
- 11.1.3. vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy;
- 11.1.4. v případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Dodavatele;
- 11.1.5. bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu; a
- 11.1.6. spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

11.2. Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických 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.

12. Řízení kontinuity činností

12.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 15 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytování Plnění na své straně:

12.1.1. zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování Plnění; a

12.1.2. pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně Plnění.

13. Kontrola a audit

13.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytování Plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle § 23 ZKB.

14. Fyzická bezpečnost

14.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 17 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytovaných Plnění na své straně:

14.1.1. dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče; a

14.1.2. 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.

15. Bezpečnostní nástroje

15.1. Dodavatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 18 až § 27 VKB, které musí splnit Objednatel. Minimálně se Dodavatel zavazuje v rozsahu poskytovaných Plnění na své straně:

15.1.1. realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě;

- 15.1.2. realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření;
- 15.1.3. připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele určenou v této Smlouvě;
- 15.1.4. bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je ve správě Dodavatele;
- 15.1.5. na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí Plnění:
- a) Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací;
 - b) Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu;
 - c) 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.;
 - d) Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejít schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT;
 - e) Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele;
- 15.1.6. připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje;
- 15.1.7. průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu poskytování Plnění a v souladu s požadavky platné české a evropské legislativy;
- 15.1.8. na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit

a jiných událostí v rozsahu poskytování Plnění dle Smlouvy, a to po celou dobu trvání Smlouvy a do dvou (2) let po jejím ukončení;

15.1.9. zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu poskytování Plnění dle Smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou;

15.1.10. pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran; a

15.1.11. veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

15.2. Dodavatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Dodavatelem narušuje chod Plnění, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato Smlouva nestanoví jinak.

15.3. Dodavatel bere na vědomí, že veškeré aktivity Dodavatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu poskytování Plnění a v souladu s interními dokumenty Objednatele, se kterými byl Dodavatel seznámen.

Příloha č.2.1-CES-datasheet-collaborative-enterprise-support

Příloha č.2.2-collaborative-enterprise-support-sla

CHECK POINT

COLLABORATIVE

ENTERPRISE SUPPORT

Check Point Collaborative Enterprise Support (CES) delivers local, personal support through a collaborative support partner who has access to our expert tools and resources and is backed by Check Point global technical assistance centers.

Collaborative Support Features

- 1st line support from a local support partner
- Global backline support from Check Point 24x7x365
- Advanced access to thousands of technical solutions and guides
- Access to the latest hot fixes, upgrades and major releases
- Prioritized routing for severe issues that demand immediate attention
- Committed Service Level Agreements with Check Point

Collaborative Support Benefits

- Work with a local support provider who understands your needs
- Maximize the value for all your Check Point products
- Proactively prevent threats before they become problems
- Strategically plan upgrades and fixes
- Submit, view and update your service requests online
- Quickly search thousands of proven solutions and documentation

CSP partners provide support in

- Canada
- United States.

CCSP partners provide support in:

- Europe
- Middle East
- Africa
- Asia
- Mexico

Choosing the right support for your Check Point solutions is essential to ensuring maximum security, connectivity, and reliability of your valuable assets. As your security needs become more complex, even a small issue can have a huge impact on your productivity and profitability—and ultimately your business success. You need local experts who speak your language and can provide onsite support, if needed. And your experts need the backing of worldwide support from Check Point teams and in-depth resources—24 hours a day—which are dedicated to providing solutions—even at the code level, if necessary. Plus, you want direct access to our large, online, self-service knowledgebase to quickly and easily answer your questions and reduce your support times and costs.

Bottom line, you want it all. Reliable support from a single point of contact, with clear visibility and accountability at every stage, dedicated to quality and your complete satisfaction so you can focus on your business—not your support.

Overview

Check Point Collaborative Enterprise Support combines the unique capabilities of local Certified Collaborative Support Provider partners with the in-depth expertise and resources of Check Point, giving you the best support available to keep your business secure.

Your local Support Provider is your point of contact for all your support issues, providing first-line support in your language with an intimate understanding of your environment and support needs. If additional support is required, your Support Provider will work directly with the Check Point global, 24x7 Technical Assistance Centers for backline support.

Our well-defined processes and documented Service Level Agreements (SLAs) ensure that we meet your expectations for quality and satisfaction.

You will receive Advanced Access to SecureKnowledge, our comprehensive self-service database designed to quickly and easily answer all your technical installation, configuration, and upgrade needs on Check Point products.

How Collaborative Enterprise Support Works

Any time you need help contact your local Support Provider first. If for some reason your Support Provider cannot solve your request, it will escalate your issue directly to a Check Point global, 24x7 "follow the sun" Technical Assistance Center. Our teams will open a service request (SR) in SecureTrak, our online service request system and then send you an email with the request details so that you can view and track your request any time. Our backline teams and engineers then work on your request, with all our resources, tools, and expertise available until we solve your issue to your satisfaction. Your CCSP is your point of contact for any support issue, giving you direct access to and clear accountability for your request. Online tools like SecureTrak give you online, up-to-the minute status of your service requests, escalated to Check Point with just one click.

Faster, more efficient resolutions

Our teams work together seamlessly to ensure that your issues reach the right resources quickly, eliminating costly delays from multiple handoffs and repetition of information. Collaborative support provides us with a deep understanding of your environment and unique needs, enabling us to resolve your issues more quickly and efficiently, increasing your satisfaction and return on investment.

Quality service from certified security experts

Collaborative Support Providers are dedicated to first-class service and support and must continually meet stringent Check Point customer satisfaction and quality requirements. All Support Providers are required to have Check Point certified Security Experts (CCSE) on staff, who are knowledgeable about the latest Check Point releases and products.

Urgent support from Check Point

Check Point offers committed response times and direct access for Severity 1 issues, defined as a problem with major system effect or system downtime. Check Point is committed to giving you, our customer, immediate support for your most urgent issues, 24x7. For Severity 1 issues, you can your program level for quality, highly available support for your mission-critical needs. Our highest-level program offers "fast path" escalation, ensuring that our senior support engineers handle your support issues at first contact.

Expanded access to online, self-service tools

You will have Advanced Access to SecureKnowledge, our self-service knowledgebase of thousands of in-depth solutions, articles, and comprehensive technical guides written by Check Point experts. Not only will you reduce your support times and resolve common issues, but you also will increase your internal skills and productivity.

Hot fixes, software updates and releases

Every level of your Collaborative Enterprise Support program includes critical software bug fixes and Hot Fix Accumulators (HFAs) to ensure continuing system maintenance and proper functionality for all your Check Point products. Software upgrades and major releases are included as part of our higher-level programs, maximizing your security with the latest applications, features, and technologies as soon as they are available.

Collaborative Enterprise Support (CES)	Co-Standard Support	Co-Premium Support	Co-Elite Support
Latest Hot Fixes and Service Packs	√	√	√
Major Upgrades/Enhancements	√	√	√
Access to Secure Knowledge	Advanced	Expert	Expert
Unlimited Service and Support	9 x 5 business days	24 x 7 every day	24 x 7 every day
Committed Response Time	4 hours	30 minutes	30 minutes
Support Focal Point	Support Desk Engineer	Premium Support Engineer	Premium Support Engineer

For more information about Check Point Support please visit
<http://www.checkpoint.com/support-programs-and-plans/index.html>

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
 U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

Check Point Collaborative Enterprise Support Service Level Agreement

**Worldwide Technical Services
Check Point Software Technologies Ltd.**

Updated: July 20, 2021

COLLABORATIVE ENTERPRISE SUPPORT (CES) SERVICE LEVEL AGREEMENT

This Collaborative Enterprise Support Service Level Agreement (the "SLA") is an agreement between you, the Certified Collaborative Support Provider (hereinafter "CCSP") and Check Point Software Technologies Ltd. (hereinafter "Check Point"). This SLA is intended to identify the features and define the processes involved with the delivery of various support functions to CCSP for the Software and Hardware products purchased and licensed from Check Point under this collaborative relationship.

1. DEFINITIONS:

"Advance Hardware Replacement" means a Hardware replacement service for Customers who have purchased Hardware Support, whereby after Check Point TAC approves an RMA, Check Point delivers a replacement to Customer's Site before Customer returns the faulty hardware to Check Point.

"ACE Partner" means an authorized Check Point partner who is staffed with Check Point Certified Professionals and Appliance Certified Experts (ACE) in accordance with Check Point ACE Partner requirements. A CCSP is not necessarily an ACE partner, as ACE requires obtaining a specialization to provide to Check Point appliance customers with special maintenance for hardware issues involving the replacement of an appliance within 4 hours or Next Business Day of notification of a problem.

"Activation Date" means the date a License Key is registered for activation of Software within the Check Point User Center.

"Appliance" shall have the meaning set forth in this SLA for the term "Hardware".

"Business Day" means normal working day in the time zone where the Customer is located.

"CCSE" stands for Check Point Certified Security Expert, which means a level of certification by Check Point which is recognized as the industry standard for Internet security certifications.

"CCSM" stands for "Check Point Certified Security Master" (CCSM), which is the most advanced Check Point technical credential, which validates the ability to use advanced commands to troubleshoot, configure and optimize Check Point Security Systems. To earn the CCSM, one needs to possess an active CCSE (R80 or higher) certification and achieve 2 infinity Specialist accreditations. With an active CCSE certification as well as two Infinity Specializations, the CCSM will be automatically awarded. There is a top certification "Check Point Certified Security Master Elite" (CCSM Elite), which will also be automatically awarded with an active CCSE and four Infinity Specializations.

"CCSP" shall mean the party identified as the Certified Collaborative Support Provider, who is the Certified Professional having the expertise and knowledge of customer needs to provide first-line support to customers having access to Collaborative Enterprise Support, and who will work directly with Check Point hereunder for backline support in order to address the customer's problems.

"CCTE" means a Check Point Certified Troubleshooting Expert (CCTE) who provides advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing a Check Point security environment.

"Certified Professional" means an individual who has passed the appropriate current Check Point Certification Test(s) to demonstrate technical competency. The current minimum requirement of a Certified Professional is a Check Point Certified Security Expert (CCSE™) for the current Major Release of Network Software and Check Point Certified Troubleshooting Expert (CCTE).

"Check Point" means Check Point Software Technologies Ltd., the party to this SLA with CCSP.

"Check Point CES Support Plan Descriptions" shall mean the document attached hereto as Exhibit A, which outlines the level of support to be provided to end users of the Software and Appliance products as part of the Collaborative Enterprise Support (defined below).

“Collaborative Enterprise Support (CES)” shall mean the currently marketed Check Point Software and Appliance support solution available to customers to keep their businesses secure, which combines the capabilities of first-line support of the CCSP, with the backline expertise and resources of Check Point. Information on the program, its support levels, as well as other details, is contained in Exhibit A (Check Point CES Support Plan Descriptions), and/or may be obtained directly from Check Point.

“Customer” means the party identified as the organization that has purchased a Check Point Support offering in connection with this SLA and initially identified a problem or issue with the Software or Appliance. Such customer interfaces directly with CCSP on first-line support issues with respect to Problem Resolution (defined below).

“Dead On Arrival (DOA)” means that a purchased Hardware product fails to operate substantially in accordance with published specifications due to defects in design, materials and workmanship during the first thirty (30) days from activation or no more than one hundred and twenty (120) days from the date of Check Point’s shipment of the Hardware product, whichever is less.

“Designated Contacts” shall mean the CCSP engineering resources that are Check Point Certified Professionals and are established in the User Center account associated with the Customer support contract.

“Device Number” means a unique identifier of a hardware device, which can be located in a label on a Hardware Product. Check Point uses Media Access Control (MAC) Address, Serial Number (SN), or Service Tag Number (STN) as a Device Number, depending on the type of Hardware.

“Documentation” means user and technical manuals provided by Check Point for use with the Software and Hardware.

“Endpoint Security Product(s)” means Check Point product(s) with an Endpoint device security focus.

“Enhancement” means all Software changes, including new releases, new versions, product improvements, system modifications, updates, upgrades, Service Packs, Feature Packs, field modifications, and all Hardware changes, including official Check Point Hardware product enhancements and accessories.

“Error” means an Error in the product, which degrades the product as defined by the Severity definitions, as compared to Check Point published functionality and performance specifications.

“Hardware” means a computing device and/or its component with a specific function and limited configuration ability. The Hardware is sold by Check Point for the purpose of executing the specific Check Point Software supplied with it.

“Information” means any idea, data, program, technical, business, or other intangible information, however conveyed.

“Intellectual Property” means Patents, copyrights, trademarks, and/or trade secrets whose owners have rights at law or in equity to exclude others from exploiting such property.

“Level 1 Support” means the ability to provide general pre and post-sales product information; hardware and software configuration; questions on upgrade Support; collect relevant technical problem identification information; perform base problem determination; provide basic Support on the standard products, protocols and features; replace Field Replaceable Units (FRUs) or whole Hardware units.

“Level 2 Support” means the ability to provide Level 1 Support plus the ability to resolve the majority of misconfigurations, troubleshoot and simulate complex configuration, hardware, and software problems; perform Hardware diagnostics to determine Hardware malfunction; support problem isolation and determination of product specification defects; provide lab simulation and interoperability and compatibility testing for new software and hardware releases prior to being deployed into a Customer production network; define an action plan; provide advanced Support on all products, protocols and features; have the ability to analyze traces, diagnose problems remotely, and provide Customer with complete steps to reproduce a problem.

“Level 3 Support” means the ability to provide Level 1 and Level 2 Support plus the ability to provide software enhancements such as patches and Hotfixes, fixing or generating workarounds that address software bugs; troubleshoot bugs that were not diagnosed during Level 2 Support; work with Customers to resolve critical situations, and building action plans with Customers to address complex issues.

“License Key” means code provided by Check Point, which activates the Software and enables the Software to operate.

“Major Release” means the current issuance of Software and/or Hardware that is designated by Check Point, as a change in the number or name, signifying a new product level. Hot Fix Accumulators (HFAs), Hotfixes, and/or Feature Packs do not constitute a Major Release change.

“Network Security Product(s)” means Check Point product(s) with network security focus.

“Previous Sequential Release” means Release of Software or Hardware, which has been replaced by a subsequent version of the product.

“Release” means Major Release of the same product.

“Problem Resolution” means the use of reasonable commercial efforts to resolve the reported problem. These methods may include (but are not limited to): configuration changes, patches that fix an issue, replacing a failed hardware, reinstalling the software, etc.

“Respond” means addressing the initial request and taking ownership of the issue.

“Response Time” means the amount of time elapsed between the initial contact by Customer to CCSP (indirect) or Check Point TAC (direct) (for co-Premium/co-Elite support level only) and the returned response to Customer by CCSP or Check Point support staff.

“RMA” means Return Material Authorization (RMA), the process of replacing a faulty Hardware or a component of a Hardware product. The process must be authorized by Check Point TAC.

“Service Level Agreement (SLA)” means the Service Level Agreement (SLA) that identifies the features and defines the processes involved with the delivery by Check Point of various support functions to the CCSP (and through the CCSP to the customer), as presented by this document's: (1) CES Support Term and Conditions; and (2) Exhibit A – Check Point CES Support Plan Descriptions.

“Service Request (SR)” means a single issue opened with Check Point TAC. The SR number identifies the Service Request. The format for the unique SR number can be as follows: 1-nnnnnnnnnn or 11-nnnnnnnn (“n” is a digit).

“Severity” Definitions for Network Security product(s):

“Severity 1” means

- (a) an Error with a direct security impact on the product;
- (b) an Error isolated to Software or Appliance in a production environment that renders the product inoperative or causes the product to fail catastrophically; e.g., critical system impact, system down;
- (c) a reported defect in the licensed product in a production environment, which cannot be reasonably circumvented, in which there is an emergency condition that significantly restricts the use of the licensed product to perform necessary business functions; or
- (d) inability to use the licensed product or a critical impact on operation requiring an immediate solution.

“Severity 2” means

- (a) an Error isolated to Software or the Appliance that substantially degrades the performance of the product or materially restricts business; e.g., major system impact, temporary system hanging;
- (b) a reported defect in the licensed product, which restricts the use of one or more features of the licensed product to perform necessary business functions but does not completely restrict use of the licensed product; or

- (c) ability to use the licensed product, but an important function is not available, and operations are severely impacted.

“Severity 3” means

- (a) an Error isolated to the Software or Appliance that causes only a moderate impact on the use of the product; e.g., moderate system impact, performance/operational impact;
- (b) a reported defect in the licensed product that restricts the use of one or more features of the licensed product to perform necessary business functions, while the defect can be easily circumvented; or
- (c) an Error that can cause some functional restrictions but it does not have a critical or severe impact on operations.

“Severity 4” means

- (a) a reported anomaly in the licensed product that does not substantially restrict the use of one or more features of the licensed product to perform necessary business functions; this is a minor problem and is not significant to operation; or
- (b) an anomaly that may be easily circumvented or may need to be submitted to Check Point Research and Development as a request for enhancement.

“Severity” Definitions for Endpoint Security product(s):**“Severity 1” means**

- (a) an Error with a direct security impact on the product; or
- (b) an Error isolated to Software, for which there is no reasonable Workaround, which renders the product inoperative, causing the end-point devices to fail catastrophically, affecting more than 1000 end point devices or 35% of deployed client base (in any case more than 100 affected end-point devices) within a production environment (not pre-deployment or staging) where end-point devices have been interrupted and not recovered; e.g., severe and general deployment wide system impact, systems are down, making end-point devices unable to perform (even with reduced performance) necessary business operations even after a change of, and/or addition of procedures, configurations, applications, tools and/or data.

“Severity 2” means

- (a) an Error isolated to Software, for which there is no reasonable workaround, which substantially degrades the usability of the end-point devices, restricting the usage of and/or access to one or more necessary business functions without completely restricting the use of the licensed product, affecting more than 500 end-point devices or 25% of deployed client base (in any case more than 50 affected end-point devices) within a production environment (not pre-deployment or staging) where the end-point devices and/or Software may have been interrupted but recovered, in part or completely; e.g., end-point devices are operative but with limited capacity, substantially impacting the end-point devices' ability to perform one or more necessary business functions; end-point devices and/or Software are operative, but an important product function is unavailable or not operating; end-point devices and/or Software may have been interrupted but recovered, in part or completely; inability to connect to the Internet /Intranet; or
- (b) an Error causing severe Software deployment/upgrade problems without prohibiting necessary business operations, affecting more than 500 end-point devices or 25% or more of the actual/intended client base (at least 50 devices affected); it may, or may not, be possible to circumvent the error, e.g., inability to install and/or upgrade product, without prohibiting the end-point devices ability to perform necessary business operations; or business operations are not prohibited but may run with reduced performance.

“Severity 3” means

- (a) an Error isolated to Software, for which there is a reasonable Workaround, or an Error that causes only a minor impact on the end-point client. Restriction in usage of one or more features of the licensed product with minor impact of necessary business functions. The Error can cause some functional restrictions but it does not have a critical or severe impact on operations, e.g., the end-point device is operational but may experience performance or operational limitations; or
- (b) an Error isolated to Software only affecting one or a limited number of individual end-point devices, that is not common for the installed end-point device population; it may, or may not, be possible to circumvent the error, e.g., an individual end-point device(s) is encountering issues not common for deployed end-point device client base.

“Severity 4” means a reported anomaly in the licensed product that does not substantially affect end-point ability to perform normal business operations. This is a minor problem and does not constitute any significant

limitation to products ability to allow normal business operation. An anomaly may be easily circumvented, e.g., a product cosmetic anomaly or documentation flaw; end-point devices and/or Software may have been interrupted but recovered.

“Shelf Spare Unit(s)” means Check Point Hardware unit(s) that is stored at Customer's Site and which is reserved for Hardware replacement usage only in case of failure of Customer's Hardware which is covered under Check Point On-Site Hardware Support Plan.

“Site” means the physical location where System(s) are installed as specified by Customer in Customer's User Center account.

“Software” means the object code version of the intangible information constituting one or more computer or apparatus programs and the informational content of such programs, together with any Documentation supplied in conjunction with, and supplementing such programs, the foregoing being provided to Customer by way of electronic transmission or by being fixed in media furnished to Customer.

“Software Subscription” means registered access to modifications, corrections, and/or updates to Software; including Hot Fix Accumulators (HFAs), security fixes, Feature Packs, and/ or major upgrades, provided to Customer by unlimited web download access or by mail upon Customer's request. Software Subscription is a deliverable for all Support Contracts.

“Support” means the technical telephone, web and e-mail assistance provided by Check Point to help the CCSP Designated Contact with Problem Resolution with respect to a Customer covered by a Support Plan and Hardware replacement services as set forth in this SLA.

“Support Plan” means the CES Support program offering options and benefits set forth on [Exhibit A](#).

“System(s)” means the Hardware, Software and Documentation that have been provided to Customer by Check Point or Check Point's authorized resellers/partners.

“TAC” means Check Point Technical Assistance Center, which is staffed by Check Point Support personnel providing assistance with diagnosis and resolution of defects and/or failures in Check Point products.

“Workaround” means a change in the followed procedures or data to avoid error without substantially impairing use of the product.

2. SUPPORT:

A description of Check Point's CES Support offerings is set forth on [Exhibit A](#), attached hereto. Upon Check Point's acceptance of a valid purchase order, and corresponding payment for that Support offering selected, Customer will be entitled to receive Support through the CCSP, according to the features and benefits provided under that offering, subject to the terms and conditions of this SLA.

2.1 Technical Support:

For Customers covered under a Check Point CES Support offering, technical Support will be provided via the CCSP pursuant to the terms of Section 5 TECHNICAL SUPPORT. Check Point agrees to provide Support, where appropriate, to CCSP, which may include but is not limited to, the following actions:

- (a) Provide CCSP with access to product update releases, related Documentation and knowledge articles, upon general commercial release;
- (b) Provide CCSP with access to TAC Technical Representatives who will work with CCSP to diagnose customer issues, and provide Problem Resolutions, including escalating the issue through TAC management as needed.

2.2 Hardware Replacement. For Customers covered under Hardware Support, Check Point will use commercially reasonable efforts to provide Hardware replacement via the CCSP in accordance with the terms set forth in Section 4 HARDWARE REPLACEMENT.

2.3 On-site Hardware Support. For those Customers whose Hardware Support level includes an on-site service feature, the Customer will approach their CCSP for 1st level diagnosis. If the CCSP determines that the issue requires RMA replacement, the CCSP will open a Service Request on behalf of the Customer with Check Point TAC. For Appliance with Co-Premium or Co-Elite support, after a repair action plan has been defined by TAC, an RMA process will be initiated by TAC immediately. For Appliance with Co-Standard support, after TAC determines with the CCSP that the hardware issue is related to a malfunction of one of the Hardware components, and after a repair action plan has been defined, an RMA process will be initiated by Check Point TAC. For Customers whose Hardware Support levels includes an on-site service feature, Check Point will use commercially reasonable efforts to dispatch a Check Point Certified On-site Technician or ACE Partner to the Site in accordance with the terms and timeframes of such plan as set forth on Exhibit A. On-site Hardware Support is effective one (1) month from the day it was purchased. Provision of on-site support is subject to the following limitations:

- (a) On-site Hardware Support is limited to Advance Hardware Replacement only, and does not include on-site service for Software troubleshooting or any Software related issues.
- (b) On-site Hardware Support may not be available for some Check Point Hardware products or in some geographic regions, and may require a set-up period before it can be made available to Customers. During such set-up period, Check Point will use commercially reasonable efforts to provide to Customer the closest available service then available, with respect to such product line or in such geographic region. Changes may apply outside of Check Point's normal service area.
- (c) On-site service response times may be dependent upon the Customer's Site address for the Hardware, the timely arrival of replacement parts at Customer's Site, and accessibility to the Site.

Note: For full unit replacement, a technician will verify that the current base software image and hotfix level are installed and will restore a backup of the machine only if the prerequisite software image dependencies are preinstalled and the backup files are available onsite and handy.

2.4 On-site Software Support for Critical Severity 1 Issues. For those Customers covered under Co-Elite Support, the Customer, or CCSP partner on behalf of the Customer, shall contact Check Point TAC directly by telephone or live chat. After TAC confirms that the matter is a Severity 1 issue, TAC and the Customer will work diligently, with highly skilled, experienced engineers to resolve the critical situation and to restore operation. In the case the criticality of the issue remains or no progress is made, after four (4) hours, Check Point will use commercially reasonable efforts to dispatch a local engineer to Customer's Site. If no local resources are available, travel arrangements will be made for the next available flight to the Customer's Site. The engineer will remain on site until the issue is no longer defined as critical (an acceptable resolution or workaround was achieved) or up to three (3) days, with travel and expense included. Provision of on-site critical Severity 1 case support under Co-Elite Support is subject to the following limitations:

- (a) A Co-Elite Customer is entitled up to three (3) visits on-site a year as required to resolve critical Severity 1 cases.
- (b) For any additional days on site that is required after the first 3 days, will be charged at a discounted rate of \$2,000 per day.
- (c) On-site critical case Support is limited to Software Support only, and does not include on-site service for Hardware issues and Hardware replacement. For On-site Hardware Support, please refer to Section 2.3 Onsite Hardware Support and Appliance Support SLA options as set forth on Exhibit A.
- (d) On-site critical case Support may not be available for some Check Point Software products or in some geographic regions, and may require a set-up period before it can be made available to Customers.
- (e) For Co-Elite support service for critical issues which requires fast arrival to the site, Check Point will cover all locations which are accessible within 12 hour elapsed commercial travel time from G7 countries hubs (US (mainland), UK, Germany, Italy, France, Japan, and Canada). In some remote locations, entry certifications requirements might add additional time to the engineer arrival on site.
- (a) Co-Elite support is account based and requires that the entire User Center install base be covered by the Co-Elite SLA. Co-Elite may not be applied to cover only portions of the User Center's products.
- (b) It is necessary that the Co-Elite Customer and the CCSP commit the necessary resources around the clock (24x7) in working with Check Point towards Problem Resolution of Severity 1 Errors.

For Severity definitions for Network Security Product(s) or Endpoint Security Product(s), refer to Section 1 DEFINITIONS, "Severity" Definitions for Network Security Product(s) and "Severity" Definitions for Endpoint Security product(s).

2.5 Support Lifecycle.

- (a) Check Point provides a comprehensive support lifecycle for its Software and Hardware. Support lifecycle policy is available at URL: <http://www.checkpoint.com/services/lifecycle/>.
- (b) Check Point will provide End of Support notification for discontinued Software to CCSP and Customer through an announcement posted on the Check Point Software Support Timeline website at URL: <https://www.checkpoint.com/support-services/support-life-cycle-policy/>.
- (c) Check Point will provide the date of Check Point's new appliance availability announcement and End of Support notification for discontinued Hardware to CCSP and Customer through an announcement posted on the Check Point Appliance Support Timeline website at URL: <https://www.checkpoint.com/support-services/support-life-cycle-policy/>.
- (d) Check Point reserves the right to modify Support Lifecycle policy at any time; notifications regarding changes in policy will be posted on the websites in Section 2.5 (b) and 2.5 (c).

2.6 Nonconformance. If Check Point determines the problem is due to nonconformance to published specifications of a Software version, or another substantial Check Point related problem, then under Check Point's Support plan, Check Point will provide any Software fix for the reported nonconformance that may be available at the time the problem is reported. If there no such fix is available, Check Point will use commercially reasonable efforts to remedy such nonconformance, which may include a Workaround or other temporary fix to the Software. If a Workaround or other temporary fix to the Software is provided, Check Point shall make reasonable commercial efforts to include it in a subsequent Software updates.

2.7 Exclusions.

Support does not include the following items or actions:

- (a) Step-by-step installation of Software or Service Packs;
- (b) Onsite services (unless Customer's level of Support, as purchased, includes this feature), Professional Services, or Educational Services;
- (c) Modification of software code, security-policy configuration, audits, or security design.

Check Point shall have no obligation to Support:

- (a) An altered, damaged, or modified product or any portion of the product incorporated with or into other software, hardware, or products not specifically approved by Check Point;
- (b) Product problems caused by Customer negligence, misuse, or misapplication, or use of the product other than as specified in the Check Point user manual, or any other causes beyond the control of Check Point;
- (c) Product installed on any computer hardware that is not supported by Check Point;
- (d) Product not purchased from the Check Point Price List.
- (e) Products subjected to unusual physical or electrical stress, misuse, negligence or accident, or used in ultra-hazardous activities;
- (f) Products that are past their End-of-Support date, as provided in Section 2.5 above.

Check Point shall have no obligation to provide Support if:

- (a) Appropriate payment for Support has not been made; or
- (b) Customer annual Support term has expired without renewal.

2.8 Reporting Non-Check Point Errors to Partner. Upon working the Service Request under normal processes, and with appropriate management review, if at that point Check Point believes that a problem reported by the CCSP may not be due to an error in the Check Point product, Check Point will notify the CCSP. At that time, the CCSP may: (a) instruct Check Point to proceed with problem determination at CCSP's possible expense as set forth herein; or (b) instruct Check Point that CCSP does not wish the problem to be pursued at CCSP's possible expense.

If CCSP requests that Check Point proceed with problem determination at CCSP's possible expense and Check Point determines that the error was not due to the error in the product, CCSP shall pay Check Point, at the Check Point then-current standard consulting rates, for all work performed in connection with such determination, plus reasonable related expenses incurred therewith. CCSP shall not be liable for:

- (a) problem determination or repair to the extent the problems are due to anomalies in the Check Point product; or
- (b) work performed after the CCSP has notified Check Point that it no longer wishes problem determination to be continued at CCSP's possible expense (such notice shall be deemed given when actually received by Check Point).

If CCSP instructs Check Point that it does not wish the problem pursued at CCSP's possible expense or such determination requires effort in excess of CCSP instructions, Check Point may, at its sole discretion, investigate the anomaly with no liability thereof.

3. CCSP AND CUSTOMER OBLIGATIONS:

3.1. CCSP Requirements. It is required that CCSP provide 24x7 Service and Support operation, and allow Customer to open unlimited Service Requests for Service and Support. CCSP shall commit to the following: (i) 30 minute response time to Customer for Severity 1 issues (note that in the case of a Co-Elite Customer, both Severity 1 and Severity 2 issues shall require a 30 minute response time); and (ii) a minimum 4-hour response time for all other issues. CCSP shall have the ability to provide Level 1 & Level 2 Support Services, and for those Customers having an onsite Support feature, the ability to provide fast arrival on site.

3.2. Support Level Alignment. CCSP shall maintain alignment between the Customer, CCSP and Check Point support levels, so that CCSP will only sell to Customer the same level of support purchased from Check Point. Thus, if CCSP sells a 24x7 Customer SLA, a Co-Premium/Co-Elite level support must be

purchased by CCSP from Check Point (CCSP may not buy from Check Point a Co-Standard level support and resell it to Customer as a higher (7x24) support level).

3.3. CCSP shall be the point of contact for support issues. CCSP will perform Level 1 Support and Level 2 Support for Customers in connection with any Software and Appliance failure reported to CCSP by Customer as set forth below. When issues are escalated to Check Point (i) the Service Request will be submitted by a CCSE, CCSM or CCTE only, and (ii) the test and debug files will be according to Check Point's guidelines for diagnostics and troubleshooting.

3.4. Level 1 Support. requires CCSP to act as the initial and primary interface to the Customer and thereafter requires CCSP to perform various responsibilities such as:

- Collection of relevant information.
- Problem identification and analysis.
- Initial diagnosis.
- Troubleshooting.
- Problem Resolution, where possible.
- Request approval from Check Point TAC to authorize the RMA for Co-standard Customer, to be provided at Check Point's sole discretion, in case of hardware failure in an appliance.

3.5. Level 2 Support. requires CCSP to perform greater troubleshooting and diagnosis, and thereafter requires CCSP to perform various responsibilities, such as:

- Perform greater troubleshooting and diagnosis.
- Potentially replicating the issue in a test lab environment.
- Provide Workaround solutions to Customer issues.
- Diagnose a Hardware issue, and determine if is related to a malfunction of one of the Appliance components, and authorize the RMA in case of hardware failure in a Check Point appliance. (Not applicable to old Nokia IP Appliances with legacy Essential /Access Appliance Support).

3.6. Direct Contact. In some limited cases, Check Point may provide Support directly to Customers in order to resolve Service Requests. CCSP and Customer are expected to provide standard support information in accordance with Section 3.9 (Support Information) in order to bring resolution to an issue in a timely fashion.

3.7. Certification and Staffing. All CCSP personnel contacting Check Point for Support must be fully trained Check Point Certified Professionals with respect to both the Major Release of the Check Point Software and the current issue with which CCSP requires assistance. The CCSP certification process requires that CCSP: (i) pass annual review and audit processing guidelines, (ii) submit performance metrics to Check Point annually or upon request, and (iii) meet customer satisfaction survey criteria at least 4 out of 5.

3.7.1. Staffing CCSE /CCSM /CCSM Elite. The number of Active CCSEs/CCSMs is set forth in the table below. The term 'Active' refers to a CCSE/CCSM (or CCSM Elite) that obtains updated certification every two (2) years. CCSEs must be trained on current Major Release and supported versions. The minimum percentage of Service Requests out of the total solved by CCSP is 75%.

3.7.2 Staffing CCTE: The number of Active CCTEs is set forth in the table below. The term 'Active' refers to CCTE which obtains an updated certification every two (2) years.

3.7.3. RMA Approval Certification for Co-Elite and Co-Premium SLAs. Annual RMA rate lower than 7.5% and False Positive Rate lower than 25%.

The Collaborative Enterprise Support level that the CCSP offers for sale to customers requires that the CCSP have a minimum number of Check Point Certified Security Experts (CCSE) and Check Point Certified Troubleshooting Experts (CCTE) on staff entitled to call for technical support:

Partner Level	Check Point Certified Security Expert/Master (CCSE/CCSM)	Check Point Certified Troubleshooting Expert (CCTE)
Distributor	2	2
2 Stars	1	1
3 Stars	1	1
4 Stars	2	2
5 Stars	2	2
Elite	2	2

For example:

A 2 Stars partner with CCSP needs to complete 1 CCSE/CCSM + 1 CCTE to meet the minimum requirements for CCSP partner.

An Elite partner with CCSP needs to complete 2 CCSE/CCSM + 2 CCTE to meet the minimum requirements for CCSP partner.

3.8. Designated Contacts: CCSP agrees that contact with Check Point will be through the specified number of Designated Contacts. Designated Contacts are named contact specified as Support Contacts within the CSP User Center Account containing the CSP Support ID, and specified as named user within the associated CSP PartnerMap account. Refer to the number of approved Designated Contracts listed in Section 3.7 Certification and Staffing. The ability to add additional contact(s) may be purchased according to prevailing program guidelines.

3.9. Support Information: The following information is requested to open an issue with Check Point TAC:

- CCSP must provide Check Point's Technical Representatives with Customer details when they open Service Requests (SR), including, but not limited to, the company name, UC number, Customer name, e-mail, and phone, and the date that the Customer opened the SR with the CCSP.
- Execute debug information, divert the output to a file, and attach the file to a web request.
- Describe the hardware platform(s) involved in this issue, including the amount of memory, disk space, and NIC card types (manufacturer and model).

- Describe the operating system(s) involved in this issue, including the version number and patch level information.
- Provide a detailed description of the problem or issue, including any symptoms noted, any patterns seen and any specific error messages received.
- Log file contains relevant log errors.
- Any kind of technical information and network environment information that Check Point's TAC engineer defines as necessary to solve the issue.
- Check Point may ask for remote access to the Customer's environment where the issue occurred.

CCSP will be asked to provide or verify the information needed for the understanding and resolution of the problem. Check Point understands that due to unusual circumstances, it may not always be feasible to include all of this information. In order to provide better service to the CCSP, Check Point requests that this information and additional information (as needed), be provided as soon as possible, as access to the appropriate data and information facilitates Problem Resolution. If it is not possible to provide this information, Check Point may be hindered in the ability to bring timely resolution to an issue.

3.10. Network Access. To the extent possible, and as requested by Check Point, CCSP and Customer understand that it may be necessary to provide Check Point or its authorized Technical Representative access to the affect network environment for any Severity 1 issue, or when Check Point determines that its Technical Representative need to access Customer's network in order to remotely diagnose an issue. CCSP and Customer understand that if access is not provided as requested by Check Point, problem determination will be slower or impaired.

3.11. System Information. CCSP and Customer must provide to Check Point information for each System under a Support Plan by registering all products in the Customer's User Center Account with accurate details:

- (a) Product License Key or Device Number;
- (b) Physical Site location of the Hardware product; and
- (c) Site contact person.

If Customer physically moves any Hardware from the original Site to an other location, CCSP or Customer must inform Check Point of such change immediately with updated Site location and contact. It is Customer's responsibility to update such change in the Customer's User Center Account. Prior to Check Point's receipt of such notification from Customer, Check Point shall not be liable for any lapses in service coverage or Hardware delivery delays with respect to such Hardware.

3.12. Backup and Removal of Data.

To reconstruct lost or altered Customer files, data, or programs, Customer must maintain a separate backup system or procedure that is not dependent on the Software or Hardware products under Support.

Where applicable, before receiving Hardware Replacement Services or before disposal or return of Hardware to Check Point, CCSP and Customer agree to:

- (a) backup and secure all programs and data contained in the Hardware;
- (b) securely erase all programs and data not provided by Check Point with the Hardware product. CCSP and Customer acknowledge that, to perform its responsibilities under this Replacement Service, Check Point may ship all or part of the Hardware product or its Software to third party locations around the world, and CCSP and Customer authorize Check Point to do so; and
- (c) remove all features, parts, options, alterations, and attachments not provided by Check Point with the Hardware product, and ensure that the Hardware is free of any legal obligations or restrictions that prevent its exchange.

3.13. On-site Access. Where applicable, CCSP and Customer agree to provide Check Point or its authorized partner with sufficient and safe access to Customer's facilities in order to permit Check Point to fulfill its obligations.

3.14. Customer Survey. Upon request by Check Point, CCSP shall provide Check Point with a list of its customers under support for the purpose of customer satisfaction survey. Check Point reserves the right to directly contact Customer for the purpose of soliciting Customer feedback about the CCSP in order to ensure the quality and consistent delivery of Support services by CCSP.

4. HARDWARE REPLACEMENT:

4.1 Hardware Return Procedure. If a Hardware product or one of its component parts does not function during the Hardware Support period, and such nonconformance can be verified by Check Point, Check Point, at its election, will provide Advance Hardware Replacement service with a refurbished part /unit for the Hardware under the type of Hardware Support Plan Check Point designates for that Hardware. A defective Hardware product or one of its component parts may only be returned to Check Point upon Check Point's prior written approval. Any such approval shall reference a Returned Material Authorization ("RMA") number issued by an authorized Check Point service representative. To request an RMA number, CCSP must contact Check Point TAC and open a Service Request. Customer should always register the Hardware Product in Customer's Check Point User Center account. If Customer does not register the Hardware Product with Check Point, Customer may be required to present proof of purchase as evidence of entitlement to Hardware Support service. The Hardware Product's Device Number will be required for all RMA cases.

Transportation costs, if any, incurred in connection with the return of a defective item to Check Point shall be borne by Customer. If such RMA Service orders are covered by Standard On-site, Premium On-Site or Elite On-Site SLA, then for the return of the defective item, Check Point will provide prep-paid shipment labels and customer will arrange pick-up of the defective item with the respective shipment service provider. Any transportation costs incurred in connection with the redelivery of a repaired or replacement item to Customer by Check Point shall be borne by Check Point.

4.2 Hardware Replacement Procedure. For Customers who have purchased Support for their Hardware, upon a suspicion of a Hardware related issue, the Customer will approach their CCSP for 1st level diagnosis. If the CCSP determines that the issue requires RMA replacement – the CCSP will open a Service Request on behalf of the Customer with Check Point TAC. For Appliance with Co-Premium or Co-Elite support, Check Point TAC will process RMA immediately. For Appliance with Co-Standard support, Check Point will attempt to diagnose and resolve problem over the phone or web. Upon determination that the Hardware issue is related to a malfunction of one of the Hardware components, an RMA process will be initiated by Check Point TAC. Check Point TAC will either issue a replacement of the faulty part (like Power Supply, Fan, Hard Disk, etc.) or a full Unit Replacement. Check Point will send the required hardware to the Site location, as it appears in Customer's User Center and as verified with CCSP when opening the Support Service Request, in accordance with the Hardware Support Plan Check Point designates for that Hardware.

Customer must ship back the faulty Hardware product (or replaceable unit) suitably packaged according to the guidelines, as specified by Check Point in the RMA letter shipped with the replacement, to a location that Check Point designates. Return shipment of the faulty Hardware should be made within five (5) business days of the arrival of the replacement or approval of the RMA for Shelf Spare Unit usage, or pay standard Check Point list price of replacement for any Hardware.

4.3 Dead on Approval (DOA). If a defective Hardware product covered under warranty fails to operate within thirty (30) days from its activation, or no more than one hundred and twenty (120) days from the date of Check Point's shipment of the Hardware product, whichever is less, Check Point will provide expedited replacement of a new unit within two (2) business days from Check Point fulfillment hub, following confirmation of any such failure. Customers outside of the fulfillment hub region should allow for additional transit time due to international customs clearance.

5. TECHNICAL SUPPORT:

5.1 **Web-based Support.** Check Point web-based Support available at URL: <https://support.checkpoint.com> provides the CCSP and Customer access to:

- (a) **Documentation**, containing product documentation, release notes, troubleshooting guides and technical white papers about Check Point Software and Hardware products, as releases become generally commercially available.
- (b) **SecureKnowledgeSM**, a self-service knowledge base, restricted repository of thousands of technical documents as well as tools covering everything from planning installation and upgrades, to understanding error messages and fixing specific known issues. Technical solutions, how-to's, and troubleshooting documents written by Check Point engineers and technical staff are added daily. CCSPs have Expert Access in accordance with the specifications of this SLA. Customers have Advanced or Expert Access in accordance with their support plan and the specifications on this SLA. When a solution is identified to solve an issue, Check Point TAC may share this solution with CCSPs via email or verbal communication.
- (c) **Software Subscription Downloads**, restricted download site for the use of the CCSP and the Supported Customers; includes latest product upgrades, Hot Fix Accumulators (HFAs), Feature Packs, security fixes, tools, and utilities for the contract term. Software Subscription guarantees that Check Point solutions are kept as current as possible through the latest product enhancements and capabilities. For Major Product releases, CCSPs and Customers may request Check Point to ship a Media Kit that includes Software upgrade package.
- (d) **Product Forums**, containing shared knowledge of Check Point products and solutions within an online community of customers, partners and employees, as well as news on Check Point products and technologies. Support Partners can view and post on the discussion threads in all Forums.

5.2 Contact TAC. CCSP's access to TAC should be either by telephone, by web request, or by live chat. CCSP's engineer's email address must be provided as well as the account details of the Customer on which behalf this ticket is opened. Once TAC verified CCSP's engineer is a CCSP Partner's Certified and Designated Contact and Customer's account has a valid Support contract, TAC representative or system will inquire information about the issue and create a Service Request in the Check Point database.

(a) **By Telephone:** Contact the nearest TAC (refer to URL: <http://www.checkpoint.com/services/contact/index.html>). An Automatic Call Distribution System (ACD) will prompt CSP to select a product group. Once CSP chooses the support option, CSP will be directed to appropriate TAC Technical Representative.

(b) **By Web Request:** Log into User Center, under the "Support" Tab, select the "Create Service Request" link. Complete the request form with all of the appropriate information about the issue and submit the request. A Service Request will be generated in the Check Point database.

PLEASE NOTE: DO NOT submit a Service Request for a Severity 1 issue via the Web request form. For a Severity 1 case, please contact Check Point by telephone and select the appropriate options for your support.

(c) **By Live Chat:** Log into User Center, under the "Support" Tab, select "Live Chat" icon. Live Chat is for quick and simple questions about Check Point products and services. Any issue requires troubleshooting must be submitted by telephone or by web request.

(d) **By Email:** Check Point does not allow opening a Service Request via email. All requests should be opened by Telephone or by web request. Correspondence on an open Service Request may be made via email, as long as the Customer Designated Contact writes a reply to emails received from Check Point TAC.

TAC access is intended to supplement the CCSP senior technical staff in accordance with Section 3 (CCSP and Customer Obligations).

Availability and accessibility of TAC is in accordance with the specifications of this SLA, subject to the situations set forth in Section 8.1 Force Majeure.

	Co-Standard	Co-Premium	Co-Elite
TAC Availability	7x24 Every Day	7x24 Every Day	7x24 Every Day
Unlimited Service Requests	Yes	Yes	Yes

5.3 Technical Support Procedures. Under Check Point's CES Support plan, Check Point TAC utilizes a multi-tier support model for Problem Resolution. When initial contact with TAC is made, a Technical Representative or Web Service Request Tool will validate CCSP and Customer information, contract information, Device Number, and gather details relevant to the question or issue. A unique Service Request (SR) number will be assigned and delivered to the Partner Certified Professional Contact, either verbally, via Web request, or via email. This SR number will be used to track any given issue from initial contact to final Problem Resolution. If appropriate, an issue will be reproduced in the Check Point Test Lab. Additional testing and problem duplication may take place in a network laboratory environment. Further investigation, including additional troubleshooting or debugging activity may be required. Based on the results of the Test Lab investigation, an issue may be resolved, or, if an anomaly is identified, elevated to the appropriate Check Point Team for final Problem Resolution.

Check Point agrees to use commercially reasonable efforts to work with the CCSP for Problem Resolution for an issue in accordance with the specifications of this SLA. Timely efforts must be made by all parties involved. If communication from Partner ceases without notice, after five (5) business days, Check Point may, upon notice, close a Service Request due to inactivity on the part of the Partner. A Service Request may be reopened within sixty (60) consecutive days of closure. Once a Service Request is closed for sixty (60) consecutive days, this issue will be considered permanently closed, and it cannot be reopened. If further

work is necessary, a new Service Request will be opened, and all pertinent materials may need to be resubmitted before work can continue.

5.4 Severity Level Response Time and Resource Commitment. Check Point agrees to use commercially reasonable efforts to respond to Partner requests based on the Severity of the issue as follows:

Severity Level	Response Time (in accordance with Support Plan)			Commitment
	Co-Standard	Co-Premium	Co-Elite	
Severity 1	30 Minutes (Indirect – 30 minute response to the CCSP)	30 Minutes (direct – Customer can contact TAC directly)	30 Minutes (direct – Customer can contact TAC directly)	Check Point and CCSP (and Customer when needed) will commit the necessary resources around the clock for Problem Resolution to obtain workaround or reduce the severity of the Error.
Severity 2	4 Hours	2 Hours	30 Minutes (direct – Customer can contact TAC directly)	Check Point and CCSP (and Customer when needed) will commit full-time resources during normal business hours for Problem Resolution to obtain workaround or reduce the severity of the Error and alternative resources during non-Standard Business Hours.
Severity 3	4 Hours	4 Hours	4 Hours	Check Point and CCSP will commit full-time resources during normal business hours for Problem Resolution, to obtain workaround or reduce the severity of the Error.
Severity 4	4 Hours	4 Hours	4 Hours	Check Point and CCSP will provide resources during normal business hours for Problem Resolution.

Note: Check Point does not guarantee the resolution of a problem within the times specified.

For Severity definitions for Network Security Product(s) or Endpoint Security Product(s), refer to Section 1 DEFINITIONS, “Severity” Definitions for Network Security Product(s) and “Severity” Definitions for Endpoint Security product(s).

The response times set forth in this Section 5.4 constitute targeted goals of the Technical Support to be provided by Check Point to CCSP, and it is understood that Check Point shall use commercially reasonable efforts to respond to CCSP requests within the target times set for the relevant Severity level. The parties acknowledge the potentially idiosyncratic nature of any issue, and agree that any sporadic failure to meet targeted times shall not constitute a breach of Check Point Support obligations under this SLA.

5.5 Escalation Process and Procedure.

- Co-Premium and Co-Elite ticket handling: Support Tickets opened for Co-Premium and Co-Elite customers will be handled by Check Point TAC’s Escalation group. After initial analysis of the issue and verification that information is sufficient and that there is no known solution to the problem at hand, the ticket will be automatically escalated to the handling of an Escalation Engineer.
- CCSP-initiated Escalation: Under Check Point’s Support plan, some work items (especially those associated with critical situations) may need to be expedited. When this becomes the case, CCSP shall notify Check Point TAC of the critical situation. If TAC determines that sufficient information has been provided by CCSP and the escalation is accepted, Check Point will work with CCSP on providing the appropriate solution. The escalation begins in accordance to Check Point standard business practices. Upon request, Check Point may provide an action plan to CCSP that may include (but is not limited by) problem statement, next action items to resolve the issue and time estimates on these action items.

- (c) Check Point Internal Escalation Process: When TAC determines an issue needs internal escalation, the issue receives a combination of increasing levels of engineering expertise and managerial attentions in accordance with Check Point standard business practice. Except for the case of a CCSP-initiated Escalation in accordance with Section 5.5 (d) below, that issue need not be escalated to a higher managerial level until the Severity of the issue increases or progress toward resolution ceases or is unduly delayed.
- (d) Management Escalation: If CCSP feels that the issue is not moving forward in an appropriate timeframe to closure, and/or an issue requires managerial attention, for immediate escalation, CCSP can either request Technical Representative to connect the CCSP to a Team Leader or contact the Team Leader of the Technical Representative handling the case directly. Team Leader's contact details are located at the bottom of the Service Request email. Regardless of the total elapsed time of an outstanding Service Request, the point of escalation shall be initiated at the Technical Representative level, escalated to the Team Leader(s), followed by TAC Manager(s), the TAC Director(s), and then the TAC Vice President. For the most current list of Check Point TAC Escalation Management contacts, refer to Escalation Management link in Service Request Web tool in the User Center.

6. LIMITATION OF LIABILITY:

NOTWITHSTANDING ANYTHING ELSE IN THIS SLA OR OTHERWISE, NEITHER CHECK POINT NOR ITS SUPPLIERS WILL BE LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS SLA UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR OTHER LEGAL OR EQUITABLE THEORY, REGARDLESS OF WHETHER CHECK POINT OR ITS SUPPLIERS WERE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR: (i) ANY PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOST DATA OR LOST PROFITS; OR (ii) FOR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY OR SERVICES; OR (iii) FOR ANY CLAIMS BASED ON ANY ERROR, DEFECT OR NONCONFORMITY IN THE PRODUCTS OR SERVICE, FOR ANY AMOUNT IN EXCESS OF THE PRICE PAID TO CHECK POINT FOR SUCH DEFECTIVE PRODUCT(S) OR SERVICE; OR (IV) FOR ALL OTHER CLAIMS NOT RELATED TO AN ERROR, DEFECT OR NONCONFORMITY IN THE PRODUCTS, ANY AMOUNTS IN EXCESS IN THE AGGREGATE OF THE AMOUNT PAID TO CHECK POINT HEREUNDER DURING THE THREE (3) MONTHS PRECEDING THE DATE THE CAUSE OF ACTION AROSE.

7. TERM and TERMINATION:

7.1 Term. Support shall be provided in annual terms and shall be renewable to the then-current Support Plan when Check Point is notified of Customer's intent to renew the existing contract, or Check Point is notified of Customer's intent to change Support Plan level. The availability of Support contract renewal is limited for products that are subject to End-of-Support notices in accordance with Section 2.5.

In order to prevent a lapse in Support, Check Point, through a reseller or CCSP support partner, must receive purchase order for renewal prior to the expiration date of a Support contract. In the event renewal made after the expiration date, Support payment terms will be back-dated to the day following the expiration date of Customer's prior contract and invoiced according to Check Point's then-current list price.

7.2 Termination. Check Point may terminate this SLA in the event Customer has not made the applicable payments to the reseller or CCSP for the designated Support Plan. Check Point shall provide a period of up to thirty (30) days to cure prior to termination.

Check Point may terminate this SLA, without liability, in the event CCSP:

- Is adjudged as bankrupt, or makes a general assignment for the benefit of its creditors, or if a receiver is appointed on account of its insolvency;
- Fails to maintain the designated number of Certified Professionals;
- Fails to solve most of the Severity 3 and 4 issues. If Support is not performed for any reason by CCSP, CCSP will work continuously to remedy the problem to the satisfaction of Check Point. Should CCSP fail to proceed with appropriate corrections to its work in an expedient manner within the timeframe set forth below, Check Point reserves the right to have the support service completed by Check Point staff or another qualified vendor, and all reasonable cost of such work shall be paid by CCSP. Check Point may elect to terminate of this SLA in accordance with this Section.

- CCSP fails to begin Problem Resolution toward a reported problem in a timely manner, fails to meet any CCSP responsibilities or obligations hereunder (and such failure or breach is not excused by Force Majeure event in Section 8.1 below) or completely cured within 5 days of the receipt of notice thereof from Check Point (or by a shorter period of time if urgent circumstances require such shorter notice), then Check Point may terminate this SLA upon the delivery of a written notice of termination to CCSP and pursue any and all remedies available at law or equity. In the event that Check Point terminates this SLA in accordance with this Section, CCSP shall be responsible for the commercially reasonable costs of having Check Point or another qualified vendor complete performance hereunder. In the event of an uncured breach by CCSP, Check Point reserves the right to assume or award the entire CCSP support service under this SLA to a third party certified professional, and until such time as such qualified vendor can be located by Check Point, Check Point may request that CCSP continue to perform its support under this SLA until its expiration or any earlier termination date as specified by Check Point in its notice to CCSP, and CCSP will work continuously with Check Point or its third party agents to carry out its work hereunder until such time period; or
- Delays under Section 20 and such delay may be prolonged.
After receipt of notice of termination hereunder, CCSP shall: (a) comply with any instructions by Check Point with respect to stopping immediately or continuing its support until the termination date designated by Check Point; (b) make no further arrangements under this SLA, except as otherwise directed by Check Point; and (c) return to Check Point all Information belonging to Check Point.

7.3 SLA Update. This SLA and related Check Point Support Plans are operational in nature and may be modified at any time by Check Point. Check Point will take appropriate measures to inform CCSP and Customer of modifications and will provide CCSP and Customer the right and window of time to review any proposed change, discuss it with Check Point, and terminate the Customer relationship without penalty if all parties cannot abide by the revisions. This SLA supersedes any previous service level agreements.

7.4 Support Plan Upgrades. Check Point permits upgrades of annual Support at any time during the term of the Support agreement. In the event a Support contract is terminated, Check Point shall not issue prorated refunds. Notwithstanding the aforementioned, in the event Check Point modifies this SLA in accordance with Section 7.3, and such modification has or will have the substantially impact on the Check Point Support Plan offered under this SLA, then the Customer may terminate said Support forthwith upon Check Point implementing any such modification and Customer may obtain a prorated refund for the remainder of the effective period.

8. Miscellaneous:

8.1 Force Majeure. Except for the obligation to pay monies due and owing, neither party shall be liable for any delay or failure in performance due to event outside the defaulting party's reasonable control, including without limitation, acts of God, earthquakes, labor disputes, shortages of supplies, actions of governmental entities, riots, war, fire, epidemics, or other circumstances beyond its reasonable control. The obligations and rights of the excused party shall be extended on a day-to-day basis for the period equal to the period of the excusable delay.

8.2 Non-solicitation. CCSP agrees not to solicit any employee of Check Point for employment, or encourage any employee of Check Point to leave his or her employment with Check Point, without the expressed written consent of Check Point. The above limitation shall be effective for the term of this Agreement and for a period of one (1) year following the termination of this SLA or any extension hereto. Solicitation does not include advertisements in the general media and, except to the extent an individual was specifically encouraged to respond to such advertisements, there shall be no restriction on the hiring of individuals so responding.

8.3 Assignment. CCSP may not assign this SLA without the prior written consent of Check Point. Check Point may transfer its rights to any wholly owned Check Point subsidiary.

8.4 Entire Agreement. This SLA, outlining the terms and conditions of Software technical support and/or Hardware replacement services for Check Point products, constitutes the entire agreement between Check Point and the CCSP and supersedes all previous written or oral agreement between the parties with respect

to the subject matter of this SLA. The terms in this SLA override any contrary terms contained in any purchase order or other CCSP documentation.

9. Office Locations:

Worldwide Headquarters:

Check Point Software Technologies Ltd.



U.S. Headquarters:

Check Point Software Technologies, Inc.



Worldwide Technical Services:

Check Point Software Technologies, Inc.



Check Point Web Site:

Check Point Support Site:

Check Point User Center:

Support Programs:

Support Services:

Support Secure FTP site:



EXHIBIT A

Check Point CES Support Plan Descriptions

Support offerings and services listed herein are subject to availability by product family and by service geographic area. Customer is advised to contact a Check Point authorized Certified Collaborative Support Partner (CCSP), or Check Point will confirm the support programs that are available for purchase at its discretion.

To contact Check Point Technical Support, please refer to URL:

1. CHECK POINT SUPPORT OFFERINGS

In order to meet the needs of its enterprise Customers, Check Point offers its Collaborative Enterprise Support program for the support of Check Point Software and Hardware products. This provides a total support service solution to enterprise/business customers through a CCSP. Below, are the program levels available under Check Point's Collaborative Enterprise Support program:

Collaborative Enterprise Support	Collaborative Enterprise Support on Appliance
• Co-Standard • Co-Standard PRO* • Co-Premium • Co-Premium PRO* • Co-Elite • Co-Elite PRO*	• Co-Standard • Co-Standard PRO* • Co-Standard Onsite** • Co-Standard Onsite PRO* ** • Co-Premium • Co-Premium PRO* • Co-Premium Onsite** • Co-Premium Onsite PRO* ** • Co-Elite • Co-Elite PRO* • Co-Elite Onsite** • Co-Elite Onsite PRO* **

*PRO support refers to enhancements to the Collaborative Enterprise Support programs which enable proactive ticket creation for severe issues, comprehensive reporting and daily monitoring of the Check Point environment.

**Onsite services refer to enhancements to the Collaborative Enterprise Support programs that deliver on-site Hardware Replacement service in case of a hardware issue is found and determined to require an RMA.

2. SUPPORT PLAN DESCRIPTION

For the most updated feature list of the Check Point Support plan, please visit the following online URL:

2.1 TAC Access.

With Check Point Software and/or Hardware Support, CCSP has access to TAC engineers per the Support plan, in accordance with the terms of this SLA, 7 x 24 - seven (7) days a week, twenty-four (24) hours a day, every day.

2.2 Support Web Access.

Access to restricted websites and resources for the sole use of the Customer and CCSP at Check Point User Center: [REDACTED] Check Point Support Center: [REDACTED]

2.3 SecureKnowledge.

Check Point provides CCSPs with access to restricted portions of its knowledgebase per the Support plan, in addition to the general installation and upgrade knowledge articles given to users with General Access. Expert Access – in addition to knowledge articles available to Customer with Advanced Access, Expert

Access contains solutions regarding issues with high fix complexity, known issues with Workarounds or Hotfixes, in-depth complex troubleshooting, and RFEs. Expert Access is given to CCSPs.

2.4 Software Subscription.

Access to restricted download site for the sole use of the CCSP and Customers; includes latest product upgrades, enhancement, Hot Fix Accumulators (HFAs), Feature Packs, security fixes, tools, and utilities.

2.5 Severity Level Response Time.

Check Point agrees to use commercially reasonable efforts to respond to CCSPs requests based on the Severity of the issue within specified time target(s) per the Support plan, in accordance with the terms of this SLA.

2.6 Support Focal Point.

Check Point Technical Assistance Centers are staffed by Support engineers who have extensive experience in supporting large-scale networks and providing assistance with diagnosis and resolution of defects and/or failures in Check Point products. As a single point of contact for all of CCSP's support needs, TAC Support engineers are grouped by expertise and experience, to ensure that TAC responds as quickly as possible by priority in accordance with the terms of the Support plan and this SLA.

- Desks Support Engineer
- Premium Support Engineer
- Escalation Support Engineer

2.7 Advance Replacement.

With Check Point Hardware Support, Customer is entitled to Advance Replacement service on the Hardware in accordance with the terms of the Support plan and this SLA. Replacement delivery targets are listed per the Support plan.

Appliance Co-Standard

After TAC determines with CCSP that the Hardware issue is related to a malfunction of one of the Appliance components, Check Point will provide Advance Hardware Replacement of the faulty Hardware Product via same business day (SBD) shipment*, with delivery target next business day (NBD).

Appliance Co-Standard Onsite

After TAC determines that the Hardware issue is related to a malfunction of one of the Appliance components, and after a repair action plan has been defined, Check Point will provide Onsite Hardware Replacement next business day (NBD), which includes delivery of replacement hardware to the Site and basic installation by a Check Point Certified Onsite Technician or ACE Partner. (For RMA determination completed by 5 pm local time).

Appliance Co-Premium; Appliance Co-Elite

After CCSP Partner determines that the Hardware issue is related to a malfunction of one of the Appliance components, and submit a Service Request for Hardware replacement with Check Point TAC, Check Point will provide Advance Hardware Replacement of the faulty Hardware Product via a customized rush service Next Flight Out (NFO) or Express Delivery shipment (when applicable**) or same day (SD) shipment, with delivery target same evening/night or early next business day (NBD) morning**.

Appliance Co-Premium Onsite; Appliance Co-Elite Onsite

After CCSP Partner determines that the Hardware issue is related to a malfunction of one of the Appliance components, and after a repair action plan has been defined by TAC, Check Point will provide Onsite Hardware Replacement within four (4) hours, which includes delivery of replacement hardware to the Site and basic installation by a Check Point Certified Onsite Technician or ACE Partner.

* For RMA determination completed by 15:00 regional hub time; otherwise shipment will occur next business day (NBD) with delivery target extended by one day.

** Next Flight Out / Express Delivery is available in the European Union and mainland USA. Appliances are shipped during normal business hours and may arrive during off hours or next business day until 9AM.