Smlouva na
Zajištění ochrany ISCS proti DDoS útokům pro PIC (primární informační centrum GŘC) a ZIC (záložní informační centrum GŘC)
č. 25/600/0340
(dále jen „Smlouva“)

uzavřená dle § 1746 odst. 2 a násl. zákona č.89/2012 Sb., Občanského zákoníku, ve znění pozdějších předpisů (dále jen „OZ“), s přihlédnutím k ustanovení § 2358 a násl. OZ, k zákonu 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“) a zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů (dále jen „ZOK“), na základě výsledku zadávacího řízení nadlimitní veřejné zakázky na služby, vedenou pod názvem „Zajištění ochrany ISCS proti DDoS útokům pro PIC a ZIC“, zadanou nabyvatelem, jako zadavatelem, v otevřeném řízení, dle § 3 písm. b), § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, (dále jen „ZZVZ“).

Smluvní strany

Česká republika – Generální ředitelství cel
se sídlem: Budějovická 1387/7, 140 00 Praha 4
IČO: 71214011
DIČO: CZ71214011
bankovní spojení: ČNB Praha 1,
číslo účtu: 1020011/0710
jednající: [redacted]
Spojení:
fax:
e-mail:
ID Dat. schránky: 7puaa4c

(dále jen „**nabyvatel**“)

a

ALEF NULA, a.s.
se sídlem: Pernerova 691/42, Karlín, 186 00 Praha 8
IČO: 61858579
DIČO: CZ61858579
společnost zapsaná: v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 2727
bankovní spojení: Komerční banka
číslo účtu: 51-3717150237/0100
zastoupená: **Ing. Milanem Zinkem**, předsedou představenstva
Spojení: [redacted]
e-mail:
ID Dat. schránky: ft2cp8u

(dále jen „**poskytovatel**“)

(nabyvatel a poskytovatel dále též společně jako „smluvní strany“ nebo jednotlivě jako „smluvní strana“).

NetScout Systems, Inc. [redacted]

Čl. 1. Předmět smlouvy

1.1 Předmět této Smlouvy je definován v Příloze č. 1 Smlouvy, a to co do množství, druhu a délky poskytnutí hardwarových komponentů a softwaru, služeb spočívajících, mimo jiné, v navrhování co nejefektivnějšího využití Systémů, v údržbě a správě Systémů a uživatelské podpoře při jejich užívání a dalšího souvisejícího plnění.

1.2 Poskytovatel se touto Smlouvou zavazuje zajistit nabyvateli užívání příslušných hardwarových komponentů a software způsobem, v rozsahu a za podmínek stanovených v této Smlouvě a též zajistit nabyvateli nezbytnou maintenance výrobce vč. zajištění DDoS testování, které proběhne 1x ročně a poskytnout technickou podporu, v rozsahu vymezeném v Příloze č. 1 Smlouvy (dále jen „Služby" a společně dále jen „plnění Smlouvy"). Smluvní strany činí nesporným, že možnost užívání software je nedílnou součástí plnění Smlouvy a že veškeré platby za plnění Smlouvy zahrnují i platby za užívání příslušného softwaru, vše, jak je definováno v příloze č. 1.

1.3 Poskytovatel se zavazuje dodat nabyvateli licenční klíče a přístupové kódy, které budou zaslány na email nabyvatele [redacted]

1.4 Předmětem dodávky a součástí plnění Smlouvy nejsou zdrojové kódy k jakémukoli softwaru.

1.5 Nabyvatel se zavazuje za řádně poskytnuté plnění uhradit poskytovateli cenu za poskytnuté plnění Smlouvy ve výši a za podmínek stanovených v této Smlouvě.

1.6 Licence k softwaru poskytovaná poskytovatelem, která je případně součástí plnění Smlouvy, je účinná od okamžiku potvrzení přijetí licenčních klíčů prostřednictvím emailu nabyvatele [redacted] na e-mail poskytovatele [redacted] a podpisu předávacího protokolu v souladu s touto Smlouvou.

1.7 Smluvní strany shodně konstatují, že na základě Smlouvy nedochází k žádnému převodu vlastnictví práv k duševnímu vlastnictví. Stejně tak nedochází na základě Smlouvy k žádnému jinému převodu vlastnického práva.

Čl. 2. Místo a doba plnění

2.1 Místem plnění předmětu Smlouvy je v případě:

a) **PIC – primární informační centrum, Budějovická 1387/7, 140 00 Praha 4,**

b) **ZIC – záložní informační centrum, Centrum sdílených služeb, s. p., Na Vápence 915/14, 130 00 Praha 3.**

Zahájením poskytování plnění Smlouvy se rozumí předání všech hardwarových a softwarových komponent plnění Smlouvy a zahájení poskytování Služeb, a potvrzení převzetí těchto komponent a počátku poskytování Služeb nabyvatelem prostřednictvím emailu. O všech těchto skutečnostech smluvní strany následně podepíší odpovídající předávací protokol. V den podpisu protokolu, dle předchozí věty, je poskytovatel povinen zahájit poskytování veškerých Služeb dle této Smlouvy a nabyvatel je povinen hradit cenu za poskytnutí plnění Smlouvy.

2.2 Poskytovatel se zavazuje zpřístupnit licenční klíče a přístupové kódy dle čl. 1. odst. 1.3 a 1.6 této Smlouvy včetně odstavce 2.1 tohoto článku a nabyvatel se zavazuje je převzít do 14 kalendářních dnů účinnosti této Smlouvy.

2.3 Dnem, od kterého je poskytovatel povinen poskytovat nabyvateli plnění dle této Smlouvy a od kterého je nabyvatel povinen hradit poskytovateli cenu za plnění Smlouvy, je den podpisu předávacího protokolu ve smyslu odstavce 2.1 tohoto článku.

2.4 Doba plnění předmětu Smlouvy je 36 (třiceti šesti) po sobě jdoucích kalendářních měsíců ode dne počátku účinnosti Smlouvy.

Čl. 3. Cena a platební podmínky

3.1 Níže uvedené ceny jsou uvedeny v Příloze č. 2 této Smlouvy.

a) Celková cena za předmět plnění Smlouvy po dobu její účinnosti činí:
6 678 000,- Kč bez DPH
8 080 380,- Kč včetně 21 % DPH
Cena za předmět plnění (poskytnutí Software vč. HW, maintenance a technické podpory v rozsahu 360 člověkohodin, DDoS testování).

b) Cena za měsíční plnění Smlouvy činí:

185 500,- Kč bez DPH
224 455,- Kč včetně 21 % DPH

3.2 Cena za případnou softwarovou část plnění Smlouvy zahrnuje též cenu přenosového média, pokud je software na něm dodáván, a veškeré náklady související s dodáním do místa plnění.

3.3 Nabyvatel uhradí cenu za dílčí plnění Smlouvy v 36 (třiceti šesti) měsíčních splátkách, a to vždy na základě odpovídajícího daňového dokladu (dále jen „dílčí faktura“) vystaveného poskytovatelem.

3.4 Smluvní cena dle odstavce 3.1 tohoto článku smlouvy je cenou nejvýše přípustnou, kterou je možno překročit jen v případě, že v průběhu účinnosti této Smlouvy dojde ke změně (snížení/zvýšení) zákonné sazby DPH. V takovém případě bude cena předmětu Smlouvy upravena (snížena/zvýšena) tak, aby odpovídala takové změně zákonné sazby DPH. O této skutečnosti není nutné uzavírat dodatek k této Smlouvě.

3.5 Dílčí faktura bude poskytovatelem vystavena nejpozději do 10 kalendářních dnů od konce měsíce, ve kterém bylo dílčí plnění Smlouvy nebo jeho jednotlivá část na základě Smlouvy poskytováno.

3.6 Splatnost řádně vystavené dílčí faktury, obsahující náležitosti dle příslušných právních předpisů, činí 30 dnů ode dne prokazatelného doručení nabyvateli do sídla uvedeného v této Smlouvě nebo do datové schránky s následujícími parametry: ID datové schránky „Generální ředitelství cel“: 7puaa4c.

3.7 Dílčí faktury musí obsahovat náležitosti daňového dokladu podle § 435 OZ, podle § 7 ZOK, podle zákona č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů a podle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“) a odkaz na tuto Smlouvu.

3.8 Dílčí faktura musí obsahovat také evidenční číslo této Smlouvy. Pokud dílčí faktura nebude obsahovat stanovené náležitosti dle této Smlouvy, nebo v ní nebudou správně uvedené údaje, je nabyvatel oprávněn vrátit dílčí fakturu ve lhůtě 10 (slovy: deseti) pracovních dnů od jejího prokazatelného obdržení poskytovateli, s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě bude dílčí faktura poskytovatelem opravena a nová lhůta splatnosti v délce 30 dnů začne plynout ode dne prokazatelného doručení opravené dílčí faktury zpět nabyvateli. V případě, že nabyvatel dílčí fakturu vrátí, přestože dílčí faktura je správná a předepsané náležitosti obsahuje, zůstává v platnosti původní lhůta splatnosti dílčí faktury a pokud nabyvatel dílčí fakturu nezaplatí v původním termínu splatnosti, je v prodlení.

3.9 Peněžní závazek nabyvatele se považuje za včas splněný dnem připsání příslušné částky ve prospěch účtu poskytovatele. Platba dílčí faktury bude provedena bezhotovostním převodem na bankovní účet poskytovatele, jenž je uveden v této Smlouvě.

3.10 Platby budou probíhat výhradně v Kč a rovněž veškeré cenové údaje budou v této měně.

3.11 Smluvní strany si dojednaly, že nabyvatel je oprávněn provést zajišťovací úhradu daně z přidané hodnoty ve smyslu ustanovení § 109a zákona o DPH, na účet příslušného správce daně, jestliže se poskytovatel stane ke dni poskytnutí úplaty za uskutečněné zdanitelné plnění nespolehlivým plátcem daně ve smyslu ustanovení § 106a zákona o DPH.

Čl. 4. Ochrana obchodního tajemství a důvěrných informací

4.1 Obě smluvní strany berou na vědomí, že tato Smlouva a veškerá práva, povinnosti a závazky z ní vyplývající, jsou považovány za důvěrné a smluvní strany se zavazují zachovávat o nich mlčenlivost. To neplatí, je-li poskytnutí informace třetí osobě nezbytné pro plnění závazků z této Smlouvy.

4.2 Smluvní strany tímto souhlasně prohlašují, že nepovažují za porušení ochrany obchodního tajemství ve smyslu ustanovení § 504 OZ a ustanovení § 1730 odst. 2 OZ situace, pokud smluvní strana poskytne v rozsahu nezbytně nutném důvěrné informace dle této Smlouvy svým právním, účetním nebo daňovým poradcům, za předpokladu, že jsou tyto osoby vázány zákonnou nebo smluvní povinností mlčenlivosti alespoň v rozsahu stanoveném v této Smlouvě. Za porušení nebude dále považována situace, kdy je povinnost poskytnutí informací dána právními předpisy či na základě rozhodnutí orgánu veřejné moci.

4.3 V případě přístupu k osobním údajům, které jsou v rámci plnění Smlouvy zpracovávány, se tímto obě smluvní strany zavazují k tomu, že při své činnosti budou postupovat v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 a zákona č. 110/2019 Sb., o zpracování osobních údajů, zejména:

a) přijmou taková opatření, která zajistí náležité zabezpečení zpřístupněných osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a náhodnou ztrátou, zničením nebo poškozením,

b) budou se zpřístupněnými osobními údaji nakládat pouze v rozsahu nezbytně nutném k plnění předmětu díla,

c) budou zachovávat mlčenlivost ohledně zpřístupněných osobních údajů,

d) v případě zapojení třetí strany do plnění předmětu díla je poskytovatel povinen tuto stranu smluvně zavázat k plnění výše uvedených povinností v oblasti ochrany osobních údajů.

Čl. 5. Servisní a reklamační podmínky, řešení vad a záruky

5.1 Počínaje dnem převzetí předmětu plnění Smlouvy nabyvatelem dle čl. 2. odst. 2.3 této Smlouvy odpovídá poskytovatel za funkčnost hardwarových komponent poskytovaných v rámci plnění Smlouvy, tak jak jsou vymezeny v příloze č. 1 s tím, že se dále uplatní SLA ujednání uvedená v příloze č. 3 této Smlouvy.

5.2 Nabyvatel odpovídá za užívání Software v rámci plnění Smlouvy v souladu s SLA ujednáními ve smyslu přílohy č. 3 této Smlouvy či na základě samostatného ujednání nabyvatele a poskytovatele.

5.3 Případné reklamace nebo nároky z odpovědnosti za vady plnění Smlouvy nebo ze související odpovědnosti za škodu bude uplatňovat nabyvatel přímo vůči poskytovateli v souladu s postupem uvedeným v příloze č. 3 této Smlouvy.

5.4 Poskytovatel se zavazuje garantovat dostupnost pro opravy, odstraňování závad a upgrade plnění Smlouvy v souladu s přílohou č. 3 této Smlouvy.

Čl. 6. Sankční ujednání

6.1 Pro případ prodlení nabyvatele se zaplacením dílčí faktury je nabyvatel povinen zaplatit poskytovateli úrok z prodlení dle nařízení vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob a evidence svěřenských fondů a evidence údajů o skutečných majitelích, ve znění pozdějších předpisů.

6.2 V případě prodlení poskytovatele se zahájením poskytování plnění Smlouvy vzniká nabyvateli nárok na smluvní pokutu ve výši 0,05 % (slovy: pět setin procenta) z celkové ceny plnění za 36 měsíců, za každý započatý den prodlení.

6.3 Při nedodržení lhůt dle čl. 5. odst. 5.4 této Smlouvy vzniká nabyvateli v případě lhůt vymezených v hodinách nárok na smluvní pokutu ve výši 500,- Kč (slovy: pěst set korun českých) za každou započatou hodinu prodlení a v případě lhůt vymezených ve dnech vzniká nabyvateli nárok na smluvní pokutu ve výši 10 000,- Kč (slovy: deset tisíc korun českých) za každý započatý den prodlení.

6.4 Žádná ze smluvních stran neodpovídá za škodu způsobenou porušením svých povinností vyplývajících z této Smlouvy, bylo-li způsobeno okolnostmi vylučujícími odpovědnost ve smyslu ustanovení § 2913 odst. 2 OZ.

6.5 Sankce i náhrada způsobené škody jsou splatné do 30 kalendářních dnů ode dne doručení písemné výzvy k zaplacení společně s příslušným daňovým dokladem – fakturou smluvní straně, která je povinná příslušnou sankci nebo náhradu škody zaplatit.

6.6 Není-li dále stanoveno jinak, zaplacení jakékoliv sjednané smluvní pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky a rovněž jí nezbavuje povinnosti uhradit náhradu škody vzniklé v souvislosti s porušením jejího závazku v plné výši. Dále si smluvní strany výslovně ujednaly, že v případě porušení dle odstavce 6.1 tohoto článku odpovídá výše úroků náhradě škody.

6.7 Smluvní strany si výslovně ujednaly, že k jiným než v tomto článku uvedeným a dále např. ústně sjednaným smluvním sankcím, jakož i k smluvním sankcím sjednaným dodatečně, nebude přihlíženo.

6.8 Smluvní strany si vyloučily aplikaci ustanovení § 1806 OZ, tzn. že úroky z úroků nelze požadovat.

Čl. 7. Rozhodné právo a řešení sporů

7.1 Práva a povinnosti smluvních stran vyplývající z této Smlouvy se řídí zejména OZ.

7.2 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě Smlouvy nebo v souvislosti s ní, včetně sporů o její výklad či platnost a usilovat se o smírné vyřešení těchto sporů nejprve prostřednictvím jednání kontaktních osob nebo pověřených zástupců.

7.3 Smluvní strany podle § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů určují jako místně příslušný soud Obvodní soud pro Prahu 1; v případě, že podle procesních předpisů je k rozhodování věci v prvním stupni příslušný krajský soud, určují smluvní strany jako místně příslušný soud Městský soud v Praze.

Čl. 8. Trvání Smlouvy

8.1 Tato Smlouva nabývá platnosti dnem jejího uzavření a účinnosti dnem uveřejnění v registru smluv. Smlouva se uzavírá na dobu 36 (třiceti šesti) po sobě jdoucích kalendářních měsíců.

8.2 Smluvní strany si výslovně ujednaly, že nabyvatel není oprávněn tuto Smlouvu vypovědět po dobu poskytování plnění Smlouvy v souladu se Smlouvou.

8.3 Nabyvatel i poskytovatel jsou oprávněni od této Smlouvy odstoupit v případě jejího podstatného porušení druhou smluvní stranou. Odstoupení se provádí písemným oznámením a je účinné jeho doručením na adresu uvedenou v této Smlouvě.

8.4 Za podstatné porušení se považuje:

a) ze strany poskytovatele prodlení při plnění termínu předání Software stanoveného v čl. 2. odst. 2.1 této Smlouvy delší než 30 (slovy: třicet) dnů,

b) ze strany nabyvatele zejména prodlení při hrazení smluvní ceny poskytovateli delší než 30 (slovy: třicet) dnů a/nebo porušení kterékoliv technické či jiné podmínky vztahující se k plnění Smlouvy, které jsou uvedeny ve Smlouvě, zejména v její příloze č. 3 této Smlouvy.

Čl. 9. Závěrečná ustanovení

9.1 Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy a nahrazuje veškerá předešlá ujednání smluvních stran ústní i písemná.

9.2 Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě vzestupně číslovaných dodatků této Smlouvy, podepsaných za každou smluvní stranu osobou nebo osobami oprávněnými zastupovat jménem smluvních stran. Smluvní strany si dále ujednaly, že k jiným formám nebude přihlíženo a nebudou jimi vázány.

9.3 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, nevyplývá-li z donucujících ustanovení právních předpisů jinak. Smluvní strany se zavazují takové neplatné či nevynutitelné ustanovení nahradit platným a vynutitelným ustanovením, které je svým obsahem nejbližší účelu neplatného či nevynutitelného ustanovení.

9.4 Smluvní strany se zavazují, že veškeré spory, které mezi nimi vzniknou, budou řešit primárně smírnou cestou (dohodou). Pokud nedojde k dohodě, budou spory řešeny věcně a místě příslušnými obecnými soudy České republiky.

9.5 Poskytovatel se zavazuje, že po celou dobu účinnosti této Smlouvy bude mít sjednanou účinnou pojistnou smlouvu pro případ způsobení škody v souvislosti s výkonem předmětné smluvní činnosti s limitem pojistného plnění v minimální výši 20 000 000,- Kč, kterou kdykoliv na požádání předloží zástupci nabyvatele k nahlédnutí.

9.6 Pro případ, že kterékoliv ustanovení této smlouvy se v budoucnu stane neúčinným nebo neplatným, smluvní strany se zavazují bez zbytečných odkladů nahradit ho novým ustanovením.

9.7 Smluvní strany si ujednaly, že závazky vyplývající z této Smlouvy se promlčují ve lhůtě 10 let ode dne, kdy smluvní strana mohla poprvé toto právo uplatnit.

9.8 Poskytovatel výslovně souhlasí s tím, že nabyvatel tuto smlouvu uveřejní na svém profilu v plném znění v souladu se ZZVZ.

9.9 V souladu se zákonem č. 340/2015 Sb. o registru smluv, se smluvní strany dohodly, že nabyvatel zašle tuto Smlouvu správci registru smluv k uveřejnění ve lhůtě, stanovené tímto zákonem. Osobní údaje smluvních stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů.

9.10 Smluvní strany si výslovně ujednaly, že tuto Smlouvu nelze postoupit na řad. Žádná ze smluvních stran není oprávněna vtělit jakékoliv právo plynoucí jí ze Smlouvy nebo z jejího porušení do podoby cenného papíru.

9.11 V případě rozporu mezi touto Smlouvou a jejími přílohami, případně dalšími podmínkami užívání předmětu Smlouvy, má vždy přednost ustanovení této Smlouvy.

9.12 Obě smluvní strany podpisem této smlouvy potvrzují, že touto smlouvou kompletně upravily svá vzájemná práva a povinnosti a vylučují, aby nad rámec výslovných ustanovení této smlouvy a jejích příloh byla dovozována jakákoliv jejich práva či povinnosti.

9.13 Smluvní strany obdrží po jednom elektronickém originálu uzavřené Smlouvy.

9.14 Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1: Technická specifikace

Příloha č. 2: Krycí list nabídky

Příloha č. 3: Licenční podmínky, Technické podmínky a SLA ujednání (přiloží poskytovatel ze své nabídky)

Příloha č. 4: Seznam členů realizačního týmu (přiloží poskytovatel ze své nabídky).

Nabyvatel

V Praze dne _____

[redacted]

Poskytovatel

V Praze dne 11.8.2025

Ing. Milan Zinek

Digitally signed by Ing. Milan Zinek
Date: 2025.08.11 14:04:30 +02'00'

ALEF NULA, a.s.
Ing. Milan Zinek
Předseda představenstva

Příloha č. 1 – Technická specifikace předmětu veřejné zakázky

Technické požadavky

Zadavatel v rámci ochrany infrastruktury před volumetrickými DDoS útoky využívá služby poskytovatele internetové konektivity T-Mobile založené na technologii Arbor. Vzhledem k tomu, že optimálního automatizovaného zabezpečení lze dosáhnout pouze kombinací lokálního boxu s nadřazenou službou, musí být nabízené zařízení kompatibilní se službou Cloud Signaling navázanou na mitigační systém Arbor Sightline, který je poskytován v rámci konektivity.

Zajištění ochrany ISCS proti DDOS útokům			
	POŽADAVKY KUPUJÍCÍHO	**NABÍDKA PRODÁVAJÍCÍHO**	
	DDOS ochrana	**Zde vyplňte splnění požadavku a popis splnění**	
PČ	DDOS ochrana ISCS slouží k monitorování a ochraně síťových zařízení a serverů ISCS před útoky z Internetu, jejichž cílem je odepření dostupnosti ISCS.	Splňuje (Ano/Ne)	Popis skutečného naplnění požadavku
	Požadované vlastnosti:		
1	Funkcionalita ochrany informačních systémů Celní správy (ISCS) je zaměřena primárně na ochranu perimetru ISCS.	ANO	Zařízení je instalováno na lince k ISP před router zákazníka.
2	Zaručení dostupnosti ochrany informačních systémů Celní správy.	ANO	Budou zakoupeny dva boxy active DC/cold standby DC.
3	V případě výpadku ochrany informačních systémů Celní správy (ISCS) zabránění výpadku konektivity pro chráněná zařízení ISCS.	ANO	Zajišťuje hardware bypass NIC.
4	Poskytnutí okamžité ochrany proti hrozbám.	ANO	Inline zařízení je schopno realtime mitigace.
5	Možnost dalšího rozšíření o schopnost spravovat veškeré možnosti ochrany informačních systémů. Celní správy (ISCS) proti DDoS útokům z jednoho rozhraní.	ANO	Ano, naše řešení umožňuje budoucí rozšíření o centrální management pro správu obou boxů (AEM).
6	Poskytnutí pokročilé možnosti nastavení ochrany proti DDoS útokům.	ANO	Zařízení umožňuje detailní nastavení množství ochranných pravidel v rozmezí vrtstev L4-L7.
7	Možnost v případě volumetrického DDoS útoku velkého objemu automaticky signalizovat poskytovateli Internetu žádost o pomoc s obranou.	ANO	Zajišťuje funkcí Cloud Singaling.
8	Poskytovat ochranu proti botnetům a novým aplikačním útokům díky pravidelným aktualizacím (Součástí nabídky musí být bezpečnostní subskripce Atlas Intelligence Feed)).	ANO	Subskripce AIF je součástí nabídky.

9	Umožnit procházení detailů o síťovém provozu, a to jak v reálném čase, tak i zpětně.	ANO	Zařízení disponuje nástrojem realtime inspekce packetů a zároveň bude logovat historické informace o napadených adresách a útočnících.	
10	Umožnit vytváření reportů.	ANO	Pravidelné nebo ad hoc reporty o napadených adresách a útocích.	
11	Kapacita zařízení od 100Mbps po 40Gbps.	ANO	Zařízení umožňuje upgrade licence až do 40Gbps. Přenos dat bude podmíněn dostatečnou kapacitou interfaců.	
12	Možnost budoucího rozšíření o funkci automatického návrhu nastavení mitigací s pomocí machine learning algoritmu, který se učí z provozu během DDoS útoku. (Subskripce Adaptive DDoS).	ANO	Ano, společně s centrálním management je možné doplnit subskripce Adaptive DDoS.	
	Požadované funkce:			
13	Dodavatel musí zajistit dodávku nového zařízení ISCS Arbor Edge Defense 8xxx včetně licencí s kapacitou zařízení od 100Mbps po 40Gbps, včetně implementace, instalace, maintenance a lokální podpory.	ANO	AE-08100-02SWA	Arbor Edge Defense. Arbor Certified software license for 2 Gbps of clean traffic
			AE-08100-02SWA-HSS	Arbor Edge Defense (AED). Arbor Certified software license for 2 Gbps of clean traffic
			A-9ANV00	Arbor Enterprise Manager licence
			Implementace a instalace jsou součástí služby včetně testování 3x za 3 roky	
14	Dodavatel musí zajistit funkčnost celkového řešení DDOS ochrany informačních systémů Celní správy (ISCS) a to sjednocením nového a stávajícího používaného řešení DDOS ochrany ISCS, které je typu Arbor Edge Defense 8xxx, pod tuto jednu smlouvu.	ANO	E-08114-HWBAA	Avnet certified HW for Netscout AED
			V rámci projektu bude sladěna podpora stávajícího řešení DDoS ochrany s nově dodávaným řešením a vše bude následně zařazeno pod jednu smlouvu.	
15	Automatická ochrana proti útokům s využitím kombinace nastavení limitů komunikace a analýzy chování, včetně maitenance a lokální podpory této DDOS ochrany.	ANO	Pomocí nastavení baseline, které se učí z provozu.	
16	Automatická ochrana proti aplikačním útokům díky pravidelně aktualizované databázi charakteristických / známých útoků (např. ATLAS Intelligence Feed), včetně implementace, maitenence a lokální podpory u nového i stávajícího řešení DDOS ochrany ISCS.	ANO	Pomocí nastavení AIF feed ochran.	
17	Možnost nastavit ochranu pro specifické zařízení nebo skupinu zařízení.	ANO	Pomocí Security Groups.	

18	Možnost úpravy definic chování, které identifikuje datový tok jako škodlivý.	ANO	Pomocí Server Group rulesetů.	
19	Schopnost monitorovat chod zařízení v reálném čase.	ANO	Pomocí syslog nebo snmp.	
20	Možnost obrany proti útoku automaticky nebo ručně, dle požadavku uživatele.	ANO	Pomocí active/inactvie módů, automatizace Cloud Singalingu.	
21	Možnost provádět packet capture na zařízení.	ANO	Pomocí nástroje packet inspection.	
22	Možnost využití API pro přístup k funkcím zařízení.	ANO	REST API rozhraní.	
23	Dodávané řešení v případě „volumetrického“ DDoS útoku (útoku velkého objemu) automaticky signalizuje službě poskytovatele Internetové konektivity žádost o pomoc s obranou ve formě čištění závadného provozu technologií poskytovatele.	ANO	Bude zajišťovat funkce Cloud Signaling.	
	Maintenance & Support			
24	Dodavatel musí zajistit maintenance a podporu dodávaného nového zařízení i stávajícího používaného zařízení DDOS ochrany informačních systémů Celní správy - HW i licence na 36 měsíců a vše zahrnuto pod jednotnou smlouvu.	ANO	Položka Maintenance & Support zakoupená na dané období.	
	Podpora je realizována partnerem dodavatele v minimálním rozsahu, viz body níže:			
25	Technická podpora po telefonu a emailu.	ANO	Telefon a mail pro hlášení incidentů.	
26	Dostupnost 24x7x365.	ANO	Tým držící pohotovost 24/7.	
27	Přístup na webové stránky zákaznického portálu.	ANO	Portál na zadávání ticketů.	
28	Softwarové aktualizace.	ANO	Instalace aktuálních vydaných SW verzí.	
29	Zajištění lokální podpory dodavatele řešení Arbor Edge Defense 8xxx.	ANO	AIF-AE-08100-02SWA-ADV-3YR	AIF subscription feed
			AIF-AE-08100-02SWA-HSS-ADV-3YR	AIF subscription feed for HSS
30	Platnost lokální podpory na 36 měsíců.	ANO	MNT-AE-08100-02SWA-T3-3YR	Maintenance for AED 8100 platform HW and SW for 36months.
			MNT-AE-08100-02SWA-HSS-T3-3YR	Maintenance for AED 8100 HSS platform HW and SW.
			MNT-A-9ANV00-T3-3YR	Maintenance for AEM
31	Dodržení SLA v rozsahu viz níže	ANO	Řešeno smlouvou o podpoře	
	Garantované časové lhůty:			
	Kategorie závady	**Response Time**	**Fix Time**	

Kritická	2 hodiny	6 hodin
Vysoká	2 hodiny	12 hodin
Střední	8 hodin	2 dny
Nízká	Následující pracovní den	1 týden
Informace	Best effort	Best effort
Kategorie servisního požadavku		**Definice kategorie servisního požadavku**
Priorita 1 **Kritická**		Zařízení Objednatele zcela selhalo nebo je rozsáhle poškozeno. Některé nebo všechny části software/softwarová aplikace podporující hlavní procesy selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je kritickým způsobem ovlivněna činnost Zařízení.
Priorita 2 **Vysoká**		Zařízení je funkční pouze částečně. Některé části software/softwarová aplikace podporující hlavní procesy selhaly a jsou zcela nefunkční nebo je jejich funkčnost omezena tak, že je zásadním způsobem ovlivněna činnost Zařízení.
Priorita 3 **Střední**		Zařízení je funkční pouze částečně. Zařízení Objednatele je výrazně ovlivněno z důvodu selhání nebo omezení některé ze systémových funkcí podporujících důležité činnosti Zařízení.
Priorita 4 **Nízká**		Zařízení je plně operativní, pouze některé funkce jsou omezeny. Tato kategorie zároveň zahrnuje funkce, které sice prokazatelně zcela selhaly, ale nejsou v daný moment využívány a nemají žádný vliv na řádný chod Zařízení. Závada má pouze zanedbatelný vliv na chod Zařízení.
Priorita 5 **Informace**		Zařízení je plně operativní, Závada je pouze kosmetického charakteru. Závada nemá vliv na činnost Systému, nebo se jedná o žádost o vysvětlení – dotaz.

Lokální podpora řešení DDoS ochrany zahrnuje kompletní škálu služeb spojenou s řešením a odstraněním technických problémů v českém jazyce. Jedná se především o tyto aktivity:			
32	Zajištění lokální podpory řešení DDOS ochrany ISCS.	ANO	Bude řešeno smlouvou o podpoře.
33	Zajištění lokální podpory nového řešení DDoS ochrany ISCS.	ANO	Bude řešeno smlouvou o podpoře.
34	Přijetí a registrace hlášení závady prostřednictvím servisního modulu dodavatele. Tento servisní modul zahrnuje kompletní škálu služeb spojenou s řešením a odstraněním SW chyb.	ANO	Bude řešeno smlouvou o podpoře.
35	On-line podpora.	ANO	Bude řešeno smlouvou o podpoře.

36	Diagnostika závad Software a diagnostika nastavení Software v místě plnění nebo prostřednictvím dálkového přístupu.	ANO	Bude řešeno smlouvou o podpoře.
37	Řešení incidentů na konfigurační úrovni Software.	ANO	Bude řešeno smlouvou o podpoře.
38	Zpřístupnění nejnovějších aktualizací SW vydaných výrobcem.	ANO	Bude řešeno smlouvou o podpoře.
39	Práce servisního experta při řešení servisních požadavků.	ANO	Bude řešeno smlouvou o podpoře.
40	Náklady na dopravu servisního experta při řešení servisních požadavků v místě plnění.	ANO	Bude řešeno smlouvou o podpoře.
41	Obnovení funkce zařízení po ztrátě systémových dat nahráním zálohy dodané kupujícím.	ANO	Bude řešeno smlouvou o podpoře.
42	Proaktivní, pravidelná kontrola Software – kontrola nastavení, bezpečnostních politik, reportů apod., konzultace.	ANO	Bude řešeno smlouvou o podpoře.
43	Profylaxe, rozšířený monitoring (performance a funkční monitoring, kontrola logů).	ANO	Bude řešeno smlouvou o podpoře.
	Požadované vlastnosti HW:		
44	Formát zařízení: HW appliance, max 2 RU dodávaná v provedení pro montáž do rackové skříně 19“ včetně veškerého příslušenství pro montáž a připojení, dle doporučení výrobce.	ANO	2RU
45	Dodávané zařízení musí umožňovat redundantní zdroje AC napájení a oba zdroje musí být obsaženy v dodávce.	ANO	2x Hot Swap 850W AC
46	Traffic Interface (Interface pro inspekci provozu) 10 Gbit LR, SM s funkcí hardware bypass při výpadku napájení.	ANO	4 x 10 GigE bypass ports LR
47	Dedikovaný Out Of Band Management port 1Gbit Ethernet a konzolový přístup RJ-45.	ANO	2 x 1Gbit Ethernet copper 1x Serial console RJ-45
	Další požadavky:		
48	Pravidelné testování funkcionality DDoS ochrany včetně ověření funkcionality služeb operátora. Test bude prováděn z vnějšího prostředí a bude simulovat reálné volumetrické i aplikační DDoS útoky cílené na prostředí ISCS. Úkolem bude ověření funkčnosti HW, správnosti nastavení interních boxů i nadřazených boxů operátora, včetně ověření fungování vnitřních bezpečnostních procesů GŘC i reakčního teamu operátora. Test bude prováděn minimálně 1x ročně.	ANO	Bude řešeno smlouvou o podpoře

Pozn.: Dodavatel vyplňuje žlutě označená pole.

K realizaci veřejné zakázky může být vybrán pouze dodavatel, který nabídne plnění, které splňuje všechny požadavky zadavatele uvedené v tabulce výše, tj. dodavatel, který ve sloupci „Splňuje ANO/NE“ uvede do žlutě podbarvených polí „ANO“ a ve sloupci „Popis skutečného naplnění požadavku“ uvede do žlutě podbarvených polí konkrétní způsob splnění požadavku zadavatele.

Příloha č. 2: Krycí list nabídky

KRYCÍ LIST NABÍDKY			
Nadlimitní veřejná zakázka na služby			
Název:	**Ochrana ISCS proti DDoS útokům pro PIC a ZIC**		
zadávaná v otevřeném řízení dle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů			
Zadavatel			
Název:	Generální ředitelství cel		
Sídlo:	Budějovická 1387/7, 140 96 Praha 4		
IČO:	71214011		
Dodavatel			
obchodní firma/název/jméno a příjmení:	ALEF NULA, a.s.		
sídlo/místo podnikání dodavatele:	Pernerova 691/42, Karlín, 186 00 Praha 8		
korespondenční adresa:	Pernerova 691/42, Karlín, 186 00 Praha 8		
jméno a podpis osoby/osob oprávněné/oprávněných jednat jménem či za dodavatele:	Ing. Milan Zinek		
IČO:	61858579		
DIČ:	CZ61858579		
kontaktní osoba:	[redacted]		
telefonní spojení:			
e-mailová adresa:			
bankovní spojení:	51-3717150237/0100		
malý a střední podnik ve smyslu doporučení Komise 2003/361/ES	Ne		
DPH [DODAVATEL vyplní sazbu]			**21%**
Celková nabídková cena za předmět plnění **Smlouvy po dobu 36 měsíců.**	Nabídková cena bez DPH	Výpočet DPH	**Nabídková cena včetně DPH**
	6 678 000,00 Kč	1 402 380,00 Kč	**8 080 380,00 Kč**

Nabídková cena měsíční platby po dobu 36 měsíců.	Nabídková cena bez DPH	Výpočet DPH	**Nabídková cena včetně DPH**
	185 500,00 Kč	38 955,00 Kč	**224 455,00 Kč**

Čestné prohlášení k vázanosti se Závazným vzorem Smlouvy	
Výše uvedený dodavatel tímto čestně prohlašuje, že plně a bezvýhradně akceptuje Závazný vzor Smlouvy, který tvoří Přílohu č. 2 ZD a je si vědom toho, že bude-li vybrán k uzavření Závazného vzoru Smlouvy na veřejnou zakázku, bude s ním uzavřena Smlouva v souladu s tímto Závazným vzorem Smlouvy.	
Osoba oprávněná jednat za dodavatele	
Podpis oprávněné osoby	Dne [ZDE VYPLNÍ DODAVATEL]
Titul, jméno, příjmení	Ing. Milan Zinek
Funkce	Předseda představenstva

Pozn: dodavatel vyplní žlutě vyznačená pole

Příloha č. 3: Licenční podmínky, Technické podmínky a SLA

NETSCOUT

Arbor Cloud Services Description and Terms

These Arbor Cloud Services Description and Terms **("ACS Description")** set forth the terms and conditions pursuant to which NetScout Systems, Inc., on behalf of itself and its affiliates **("Licensor")** provides Arbor Cloud Services to a customer **(an "End User")** who has purchased Arbor Cloud Services. This ACS Description is an addendum to, and supplements the terms of, the agreement which governs the End User's purchase and/or use of Licensor Products and/or Services **(the "Agreement")**. Together, the Agreement and this ACS Description govern the End User's use of, and each party's obligations with respect to, the Arbor Cloud Services. In the event of a conflict between this ACS Description and the Agreement, this ACS Description shall control with respect to Arbor Cloud Services. Capitalized terms not otherwise defined in this ACS Description shall have the meaning ascribed to them in the Agreement.

1. DEFINITIONS

The following definitions shall apply to the capitalized terms used herein.

1.1 "/24 Prefix" means a block of two hundred fifty-four (254) continuous IP addresses.

1.2 "Always On Protection Service" shall mean the services described in **Section 2.2**.

1.3 "Arbor Cloud Platform" means the integrated hardware and software combined to form the network controlled by Licensor or its hosting agent in connection with the provision of the Arbor Cloud Services, excluding telecommunications services providing a connection between any Arbor servers used in the provision of the Arbor Cloud Services.

1.4 "Arbor Cloud Services" means the cloud-based services provided by Licensor and performed by its employees or agents which "cleans" or "scrubs" certain internet-based, malicious, attack traffic from a stream of internet-based traffic directed to the End User's Endpoint and, where applicable, any supplemental services purchased by End User as described in this ACS Description.

1.5 "Attack" or "Attack Incident" shall mean an event in which malicious traffic (e.g. Distributed Denial of Service **("DDoS")**), is directed to an Endpoint which is on the Arbor Cloud Platform. The determination as to whether traffic is Attack traffic shall be determined solely by Licensor.

1.6 "AUP" shall mean the Acceptable Use Policy which is described in **Section 5.8**.

1.7 "Auto-Mitigation" shall mean a mitigation action taken automatically by the Arbor Cloud Platform upon receiving a supported triggering action that has been agreed upon by both parties and using a pre-configured default mitigation template that has been setup for End User.

1.8 "BGP-Based Services" shall mean services in which mitigation is performed by the redirection of End User traffic to the Arbor Cloud Platform via a Border Gateway Protocol **("BGP")** routing change.

1.9 "Clean Traffic" shall mean the 95th percentile peak Mbps of legitimate End User internet traffic going into or out of the Arbor Cloud Platform for an Endpoint, which is processed by the Arbor Cloud Service in accordance with the type of service purchased by End User.

1.10 "Content" shall mean all data, software, and information that End User or its authorized users provides, authorizes access to, or is contained within the traffic provided to the Arbor Cloud Services.

1.11 "DNS Based Services" shall mean services in which mitigation is performed by the redirection of End User traffic to the Arbor Cloud Platform by changing the Domain Name Service **("DNS")** record for End User hostname.

1.12 "Emergency Setup" shall mean initial provisioning of End User DNS hostname information into the Arbor Cloud Platform within an expedited timeframe as defined in **Section 2.1D** of the SLA.

1.13 "Emergency Updates" shall mean changing End User DNS hostname information in the Arbor Cloud Platform within an expedited timeframe as defined in **Section 2.1E** of the SLA.

1.14 "Endpoint(s)", as used herein, means that part of an End User's infrastructure subject to protection by the Arbor Cloud Services.

1.15 "Flow Monitoring Service" shall mean the services described in **Section 2.3**.

1.16 "Incident" means an event wherein End User has directed internet-based traffic for an Endpoint to the Arbor Cloud Platform and shall include both Attack Incidents and Non-Attack Incidents.

1.17 "Location" means, for BGP-Based Services only, End User router Endpoint to terminate Generic Routing Encapsulation **("GRE")** tunnels connected to the Arbor Cloud Platform.

1.18 "Mitigation Incident" means either (a) the event commencing when Licensor announces the Requested Prefix out of the Arbor Cloud Platform and ceases when End User contacts Licensor pursuant to then-current Licensor policies and directs Licensor to cease such announcement(s) or (b) an event where more than twenty-five (25) kilobits per second **("Kbps")** of End User traffic flows through the End User's assigned DNS Redirection VIP address on the Arbor Cloud Platform. For purposes of calculating the measurement period of a Mitigation Incident, (i) for On Demand Services, the Mitigation Incident shall be calculated for each seventy-two (72) hour period for which traffic is diverted, and (ii) for Always-On Protection Service, the Mitigation Incident shall be calculated for any consecutive seventy-two (72) hour period during the Mitigation.

1.19 "Network Flow Telemetry" shall mean digital records that are created by network devices and transmitted to a data processor over the network, consisting of metadata-based characteristics that describe data traffic connections made over a monitored network. Such characteristics include but are not limited to source and destination IP addresses, IP protocol, source and destination ports, traffic volume, timestamp, and network interfaces utilized.

1.20 "Non-Mitigation Incident" shall mean, for purposes of On Demand Services, a Mitigation Incident in which the End User has directed internet-based traffic for an Endpoint to the Arbor Cloud Platform and there has been no Attack traffic for a period of seventy-two (72) consecutive hours.

1.21 "On Demand Services" shall mean the services described in **Section 2.1**.

1.22 "Provisioning Process" means Licensor's then-current process for provisioning of an Endpoint, a change to configuration, or directing End User traffic to or away from the Arbor Cloud Platform.

1.23 "Quotation" means the document issued by Licensor under which Licensor offers for sale the Arbor Cloud Services.

1.24 "Requested Prefix" means the /24 Prefix or such other subnet prefix agreed to by the Licensor in connection with the Arbor Cloud Services being provided to End User.

1.25 "SLA" means the Service Level Agreement attached as **Exhibit A** to the ACS Description.

1.26 "Standard Setup" shall mean the initial provisioning of End User network up to 100/24 subnets and/or hostname information up to 100 DNS hostnames and/or up to 50 GRE destinations into the Arbor Cloud Platform within normal timeframes as defined in **Section 2.1B** of the SLA. Setup of direct connections into the Arbor Cloud infrastructure and BGP peering with Arbor Cloud are not included in Standard Setup.

1.27 "Standard Updates" shall mean changing End User network up to 100/24 subnets and/or hostname information up to 100 DNS hostnames and/or up to 50 GRE destinations into the Arbor Cloud Platform within normal timeframes as defined in **Section 2.1C** of the SLA. Setup of direct connections into the Arbor Cloud infrastructure and BGP peering with Arbor Cloud are not included in Standard Setup.

1.28 "VIP(s)" or "DNS Redirection VIP(s)" means, for DNS customers only, the Licensor-assigned IP address on the Arbor Cloud Platform which terminates to only one (1) End User hosted IP address to send Clean Traffic and receive outbound internet traffic.

2. DESCRIPTION OF SERVICES

The following describes the types of Arbor Cloud Services that Licensor makes generally available to its customers. The terms in this ACS Description shall apply only to the type of Arbor Cloud Service(s) actually purchased.

2.1 On Demand Services. The On-Demand Service is an on-demand service offering in which the End User can route traffic through the Arbor Cloud Platform on a per-Incident basis, subject to the terms of this ACS Description, in order for their traffic to be filtered in mitigation in the course of an Attack or threat of an Attack.

2.2 Always On Protection Services. The Always-On Protection Services shall mean the service offering in which the End User can continually route their traffic through the Arbor Cloud Platform at all times, subject to the terms of this ACS Description, independent of any Attack or threat of Attack.

2.3 Flow Monitoring Services. The Flow Monitoring Services shall mean the service offering in which Licensor shall provide monitoring services of End User's Network Flow Telemetry from End User's routers.

2.4 Service Provider Package. End User shall use the Arbor Cloud Services only for its own internal business operations; provided, however, if End User has purchased the Arbor Cloud Services as a Service Provider Package, then End User may use the Arbor Cloud Services to provide services to End User customers who access the Arbor Cloud Services using End User's network. If the Arbor Cloud Service is purchased as a Service Provider Package, then the provisions of this Section 2.4 shall apply and: (i) End User's customers must have entered into a formal contractual agreement with End User containing confidentiality provisions that incorporates terms at least as protective as those terms provided in the Agreement and that recognizes the intellectual property rights in the Arbor Cloud Services belongs to Licensor, (ii) End User will make no representations, warranty or covenant (whether express or implied) regarding the Arbor Cloud Service, (iii) and all obligations of Licensor are direct only to the End User, and

End User's customers shall have no third party beneficiary rights with respect to this ACS Description and the services provided hereunder.

3. PROVISION AND USE OF ARBOR CLOUD SERVICES

3.1 For BGP-Based Services. End User acknowledges that deployment on the Arbor Cloud Platform may require configuration which takes several days and that in such instance, any activation of Arbor Cloud Services on an expedited basis shall require deployment on the DNS-based platform rather than the BGP-based platform as Licensor, in its reasonable discretion, determines is appropriate.

3.2 For DNS Based Services. The Arbor Cloud Service may be provisioned to protect up to ten (10) ports per domain for standard TCP-based and/or UDP based application layer protocols.

3.3 Language. Where applicable, all obligations of each party, including without limitation, delivery of the Arbor Cloud Services, interfaces, support obligations or requests, and notices shall be required to be performed in English, and all interaction, whether with End User or Licensor shall be conducted using English. End User shall ensure that, during the entirety of a Mitigation Incident, End User will have available a technical contact that speaks English for interaction with Licensor's support team.

3.4 Trial Use. Licensor may make Arbor Cloud Services available for End User's use on a trial basis, to the extent set forth in the Quotation. Such Trial Services shall be subject to the terms of this ACS Description; however, the Trial Services shall not be subject to any Credits described in the SLA.

4. MITIGATION USING ARBOR CLOUD SERVICES.

4.1 Licensor shall calculate the End User's total amount of used Clean Traffic in Mbps, at the ninety-fifth (95th) percentile during each Mitigation Incident to confirm End User is within its total contracted Clean Traffic amount. Clean Traffic shall be determined by periodically measuring End User's Clean Traffic bandwidth utilization running through the Arbor Cloud Platform. At the end of a measurement period (Mitigation Incident), the utilization measurements are ordered from highest to lowest and the top five percent (5%) of the traffic measurements discarded. The next highest measurement for the inbound or outbound traffic is considered the ninety-fifth (95th) percentile Clean Traffic.

4.2 For On-Demand Service, in the event of a Mitigation Incident, any traffic which is directed to the Arbor Cloud Platform that is not for a pre-provisioned domain, protocol or port will be blocked.

4.3 For On-Demand Services, End User acknowledges that the Arbor Cloud Service is an on-demand service for use during Attack Incidents only and is not meant to be used as an always-on service during periods when an Attack is not occurring or when Licensor has not explicitly agreed to continue for another mitigation period. Any such use when an Attack is not occurring may incur additional fees in accordance with **Section 8.1**.

4.4 Attack traffic may be mitigated as far "upstream" as possible, including internet network provider access control lists **("ACLs")**, Flowspec, black hole routing or other network-based blocking mechanisms.

4.5 The Arbor Cloud Service includes Layer 4 rate limiting protection for HTTPS traffic provisioned on the Arbor Cloud Platform. The Arbor Cloud Service does not open HTTPS packets for "inspection", "cleaning" or "scrubbing" unless the End User has elected to utilize a packet inspection service, if offered, at the application Layer 7 level on a per domain, per SSL certificate basis. This packet

inspection service requires End User to provide Licensor with valid SSL certificates to be loaded on to the Arbor Cloud Platform for the traffic that shall be subject to HTTPS packet inspection.

4.6 During any Attack Incident, Licensor will work with the End User, where required, to fine tune the Arbor Cloud Services during a Mitigation Incident with a goal of achieving greater DDoS protection while minimizing traffic disruption.

5. END USER OBLIGATIONS

5.1 End User agrees that the successful and timely performance of the Arbor Cloud Services requires End User's good faith cooperation and participation, including following the guidelines set forth in Licensor's service guide for the Arbor Cloud Services. Accordingly, End User agrees to fully cooperate with Licensor including without limitation: (i) providing relevant information reasonably requested by Licensor on the Endpoints prior to the activation of the Arbor Cloud Services pursuant to the Provisioning Process with respect to each Endpoint, and during the provision of Arbor Cloud Services shall inform Licensor of any changes to such information, (ii) provide all other information reasonably requested by Licensor which Licensor determines is reasonably necessary in order to provide the Arbor Cloud Services, and (iii) take such other actions that Licensor determines is reasonably necessary to enable Licensor to perform the Arbor Cloud Services, including without limitation providing access to, and availability of, the Endpoints in order to allow the Licensor to perform the Arbor Cloud Services. In addition, End User agrees to make the necessary configuration changes to its infrastructure to enable the performance of the Arbor Cloud Services. End User acknowledges that the Arbor Cloud Services may be delayed or not completed if End User does not cooperate with Licensor, or if Licensor's performance is otherwise delayed or prevented by End User, and Licensor shall not be held accountable for any such delays as a result of End User's failure to take the foregoing actions.

5.2 For BGP-Based Services, End User must provide and utilize a BGP and GRE capable device(s) and properly configure such device(s).

5.3 For Flow Monitoring Services, End User must provide the types of Network Flow Telemetry that are specified in the service guide for the Arbor Cloud Service.

5.4 End User acknowledges that in order for Licensor to provide the Arbor Cloud Services, End User's internet traffic for the Endpoint must first be redirected to the Arbor Cloud Platform.

5.5 End User acknowledges that operation and performance of the Arbor Cloud Services involves repeated filtering of traffic to the Endpoint and End User expressly consents to the same. End User hereby grants Licensor and its agents, for the Term, a non-exclusive, non-transferable, royalty-free license to access any part of the internet traffic flowing to the Endpoint and any application traffic contained therein for the purposes described in this ACS Description.

5.6 End User shall be solely responsible for the direction of all internet traffic for an Endpoint by following Licensor's procedures then in effect under the Provisioning Process (which may include, by way of example, contacting Licensor's support team and having Licensor announce or cease announcing the Requested Prefixes or changing DNS to DNS Redirection VIPs).

5.7 End User shall provide Licensor with written instructions on the End User's escalation and authorization protocols for its emergency/incident response procedures for DDoS attacks. This information will be required to be provided to Licensor during the Provisioning Process.

5.8 End User shall comply with the following Acceptable Use Policy for Arbor Cloud Services **("AUP")**, as may be updated pursuant to section 12. End User shall not use, or allow use of, the Arbor Cloud Service in violation of this AUP, including any of the following types of abuses **("Abuses")**: (a) use of the Arbor Cloud Service in an unlawful manner or for an unlawful purpose, (b) use of the Arbor Cloud Service in a manner that, in Licensor's reasonable discretion, directly or indirectly produces or threatens to produce a negative effect on the Arbor Cloud Service network other than in a manner for which the Arbor Cloud Service network was designed or that interferes with the use of the Arbor Cloud Service network by other customers or authorized end users, including, without limitation, overloading servers or causing portions of the Arbor Cloud Service network to be blocked, or (c) with respect to On Demand Service, excessive or prolonged use of the Arbor Cloud Service while not actively mitigating a DDoS attack or incident.

5.9 Licensor may suspend an Endpoint or the Arbor Cloud Services, as applicable, if, in Licensor's reasonable determination, an Abuse occurs. Such suspension shall remain in effect until End User corrects the applicable Abuse. In the event that, in Licensor's reasonable determination, an Abuse is critically impacting, or threatens to impact critically, the Arbor Cloud Service network or servers, Licensor may suspend an Endpoint or the Arbor Cloud Service, as applicable, immediately and without prior notice. In the event that an Abuse is not critically impacting the Arbor Cloud Service network or threatening to do so, Licensor shall give prior notice of any suspension. End User's failure to correct any Abuse within thirty (30) days after receipt of notice will entitle Licensor to terminate Arbor Cloud Services effective immediately upon Licensor's delivery of the termination notice.

5.10 Licensor may discontinue the Arbor Cloud Service at any time upon seventy-five (75) days prior written notice provided that such right shall not be utilized by Licensor as a termination for convenience but shall only be used where such discontinuance would apply to all or substantially all of Licensor's Arbor Cloud Services customers and, provided that End User is not in default under the terms of the Agreement and this ACS Description, Licensor shall provide a refund of the pre-paid fees for the period after the effective date of termination.

6. CONTENT AND DATA PROTECTION

6.1 Use of the Arbor Cloud Service will not affect End User's ownership or license rights in its Content. Licensor employees and contractors may access and use the Content solely for the purpose of providing and managing the Arbor Cloud Service. Licensor will treat all Content as confidential by not disclosing Content except to Licensor employees and contractors and only to the extent necessary to deliver the Arbor Cloud Service. Licensor may use End User Network Flow Telemetry in aggregate and/or anonymized form to compile statistics related to the performance, operation, and use of the Arbor Cloud Service ("Service Statistics"), provided that the Service Statistics will not identify End User as the source of the Network Flow Telemetry. Licensor retains all intellectual property rights in the Service Statistics.

6.2 End User is responsible for obtaining all necessary rights and permissions to enable and grant such rights and permissions to Licensor employees and contractors, to use, provide, store, and otherwise process Content in connection with the Arbor Cloud Service, and by providing such Content to Licensor all such action shall be deemed by Licensor to have been obtained without the necessity for Licensor to confirm such actions. This includes End User making necessary disclosures and obtaining consent, if required, before providing individuals' information, including personal or other regulated data in such Content. End User is responsible to determine the suitability of the Arbor Cloud Service with respect to applicable laws that End User is subject to related to End User's business.

6.3 Licensor will return or remove Content from the Arbor Cloud Platform upon the expiration or termination of the Arbor Cloud Services, or earlier upon End User's request.

7. TERM AND TERMINATION

The Arbor Cloud Service shall commence on Licensor's acceptance of a purchase order from End User or authorized Licensor reseller, as applicable, and shall continue in effect for the term set forth on the Quotation **("Initial Term")**. Upon expiration of the Initial Term, the Arbor Cloud Service may be renewed upon Licensor's receipt of a renewal purchase order for successive twelve (12) month periods or for the term set forth in the Quotation **("Renewal Term(s)") (the Initial Term and any Renewal Terms, collectively the "Term")**.

8. PAYMENTS AND FEES

8.1 Service fees for the Arbor Cloud Services will be as set forth in Quotations **("Service Package Fee")**. Licensor will have no obligation to perform the Arbor Cloud Services until it receives a valid and acceptable purchase order for such services. The Service Package Fee includes the amount of traffic contracted to be covered hereunder, together with other components purchased as indicated on the applicable Quotation. Additional options may be purchased for an additional fee which will be set forth in a separate Quotation issued by Licensor at the time such additional services are requested. For purchases of Arbor Cloud Services made directly through Licensor, invoicing will be on an annual recurring basis unless otherwise specified on the applicable Quotation. All payment obligations to Licensor are non-cancelable and non-refundable unless otherwise specifically set forth herein, and the purchased Arbor Cloud Services may not be downgraded during a then-current term of the Arbor Cloud Services. Additional fees that may be charged based upon use of the Arbor Cloud Services include the following:

8.1.1 Mitigation Incident Fees. The Mitigation Incident Fee shall mean the fee that applies to a Mitigation Incident above and beyond the Mitigation Incidents that are included in the Service Package Fee. The Mitigation Incident Fee shall cover a period of up to seventy-two (72) consecutive hours or any portion thereof. Mitigation Incidents longer in duration than seventy-two (72) consecutive hours are subject to Mitigation Incident Fees for each period of consecutive seventy-two (72) hours or any part thereof. The Mitigation Incident Fees are applicable only when purchasing Arbor Cloud Service that include a limited number of mitigations.

8.1.2 Non-Mitigation Incident Fees. The Non-Mitigation Incident Fees are applicable only when purchasing Arbor Cloud Services that include unlimited mitigations and shall be in the amount of one (1) month of Service Package Fee, unless otherwise specified in the Quotation. Use of the Arbor Cloud Service when an Attack is not occurring and without prior authorization from Licensor for a period of any time up to seventy-two (72) consecutive hours is considered a Non-Mitigation Incident and may be assessed a Non-Mitigation Incident Fee at Licensor's discretion.

8.1.3 Clean Traffic Overage Fees. The Clean Traffic Overage Fee shall mean a fee that Provider reserves the right to charge in the event that the amount of Clean Traffic sent by an End User to the Arbor Cloud Platform during any combination of two or more Mitigation Incidents or the Non-Mitigation Incident exceeds the amount of Clean Traffic contracted for the specific End User, and Provider and End User fail to reach a mutual agreement on remediation. Such fee will be determined using the 95th percentile peak Clean Traffic flowing through the Arbor Cloud Platform and will be calculated for each instance in which a Mitigation Incident or Non-Mitigation Incident exceeds the then-current list price for every 100Mbps or part thereof over the contracted rate.

8.2 All Service Packages include up to two (2) Standard Updates per month of service. Other services including additional Standard Updates, Emergency Setup requests or Emergency Update requests,

must be purchased separately. Licensor shall not be obligated to commence with any additional services until it has received and accepted a purchase order for the additional services. Notwithstanding the foregoing, during emergency situations Licensor may agree to perform additional services immediately based on mutual agreement that a purchase order for such additional services will be provided within thirty (30) days following receipt of the applicable Quotation.

9. WARRANTIES

9.1 Licensor represents that the Arbor Cloud Services will perform as described in the service level agreement attached hereto and incorporated herein as **Exhibit A ("SLA")**. EXCEPT AS EXPRESSLY SET FORTH IN THIS **SECTION 9.1**, LICENSOR MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE ARBOR CLOUD SERVICES. FURTHER, LICENSOR EXERCISES NO CONTROL OVER, AND ACCEPTS NO RESPONSIBILITY FOR CONTENT OR INFORMATION CONTAINED IN THE TRAFFIC DIRECTED TO THE ARBOR CLOUD SERVICES. END USER'S SOLE AND EXCLUSIVE REMEDY, AND LICENSOR'S SOLE AND EXCLUSIVE OBLIGATION, WITH RESPECT TO THE ARBOR CLOUD SERVICES AND ANY BREACH OF THE FOREGOING REPRESENTATION IN THIS **SECTION 9.1** WILL BE THE REMEDIES SET FORTH IN THE SLA. A breach of the representation in this **Section 9.1** or the SLA shall not constitute a breach of the Agreement but shall give rights solely to the remedies and credits set forth in the SLA.

9.2 End User represents and warrants that: (a) End User has all right, title and interest or is the licensee with right to use and/or access all of the Endpoints, applications and/or Content provided to Licensor in order for Licensor to perform the Arbor Cloud Services and all of the Content accessed at End User's direction to perform the Arbor Cloud Services; (b) if the End User utilizes a packet inspection service, that its provision of the SSL certificate for the HTTPS Packet Inspection service and Licensor's use thereof for provision of the Arbor Cloud Service does not violate any laws, security policies or regulations or infringe the proprietary or privacy rights of any third party; (c) End User shall not use the Arbor Cloud Services for any unlawful purpose; and (d) End User shall comply with its obligations under this ACS Description. End User further represents that neither the U.S. Bureau of Industry and Security nor any other governmental agency has issued sanctions against End User or otherwise suspended, revoked or denied End User's export privileges. End User will defend, indemnify and hold harmless Licensor for any third-party claims, including claims made by regulatory agencies arising out of End User's use of the Arbor Cloud Services based on the Content.

10. INDEMNITY

End User will defend at its own expense any action brought against Licensor, its directors, officers, or employees by a third party to the extent that the action is based on a claim, suit, or proceeding arising from or relating to (i) the breach of any representation or warranty set forth in Section 9.2 above; (ii) any third party claim that Licensor's provision of the Arbor Cloud Service to Endpoints designated by End User in connection with performing the Arbor Cloud Services for End User is not authorized; (iii) Content, including without limitation, any claim involving alleged infringement or misappropriation of any patent, copyright, trademark, trade secret or other intellectual property right; or (iv) claims made by regulatory agencies arising out of End User's use of the Arbor Cloud Services based on the data contained within the Content. This Section 10 shall survive termination of the Arbor Cloud Services and the Agreement.

11. EXPORT REGULATION

In addition to the export controls provisions contained in the Agreement, End User will not use the Arbor Cloud Service to export or re-export any technical data or software in violation of applicable export laws. End User is solely responsible for compliance related to the manner in which End User chooses to use the Arbor Cloud Service, including End User's transfer and processing of Content and the region in which any of the foregoing occur. End User is solely responsible for ensuring that all users of End User's account are not "Denied Parties" under applicable export laws.

12. CHANGES TO THIS ACS DESCRIPTION

Licensor may make changes to this ACS Description (including the AUP and/or the SLA) at any time by posting a revised version at https://www.netscout.com/legal/terms-and-conditions and any successor site designated by Licensor. Except with respect to changes in the AUP, such changes shall apply only to purchase orders placed for the applicable Arbor Cloud Service after the aforementioned changes take effect. All changes to the AUP shall become effective immediately.

13. LIMITATION OF LIABILITY

EXCEPT FOR CUSTOMER'S INDEMNITY OBLIGATIONS HEREUNDER OR INFRINGEMENT OF LICENSOR'S INTELLECTUAL PROPERTY, NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR SPECIAL, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES OR COSTS OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR SERVICES, LOST PROFITS, LOST SAVINGS, LOSS OF INFORMATION OR DATA, OR BUSINESS INTERRUPTION, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

EXCEPT FOR CUSTOMER'S INDEMNITY OBLIGATIONS HEREUNDER, INFRINGEMENT OF LICENSOR'S INTELLECTUAL PROPERTY, OR OBLIGATION TO PAY HEREUNDER, IN NO EVENT WILL EITHER PARTY'S LIABILITY EXCEED THE AMOUNTS PAID OR PAYABLE BY CUSTOMER TO LICENSOR FOR THE SERVICE THAT GAVE RISE TO SUCH CLAIM.

EXHIBIT A TO
ARBOR CLOUD SERVICES DESCRIPTION AND TERMS SERVICE LEVEL

AGREEMENT

This Service Level Agreement **("SLA")** for the Arbor Cloud Service is attached to and made a part of these Arbor Cloud Services Description and Terms **("ACS Description")**. In the event of a conflict between the terms of the Agreement or this ACS Description and the terms of this SLA with respect to Arbor Cloud Service, the terms of this SLA shall control. Capitalized terms not otherwise defined in this SLA shall have the meaning ascribed to them in the ACS Description. All sections referred to herein shall refer to sections in this SLA unless otherwise stated.

1. DEFINITIONS

The following additional definitions shall apply to this SLA.

1.1 "Credit" shall mean the credit issued for a Service Outage and shall be the pro-rated value of one (1) day of fees determined by dividing the monthly Service Package Fees payable to Licensor by the number of days in the calendar month in which the Service Outage occurs.

1.2 "Direct Connect" shall mean a dedicated network connection between the End User owned and/or provided circuits direct into any Arbor Cloud Data Center for the purpose of returning clean traffic post an Arbor Cloud mitigation or traffic redirection event.

1.3 "Scheduled Maintenance" shall mean pre-defined periods of time where the Arbor Cloud Services may be unavailable or have degraded capacity due to the occurrence of planned system changes.

1.4 "Service Outage" shall mean a failure of the Arbor Cloud Service to meet the applicable Service Levels set forth in **Section 2.1** for the relevant Arbor Cloud Service, and no exception described in **Section 2.3** applies.

2. SERVICE LEVELS

2.1 A Service Outage, subject to **Sections 2.2 and 4.2** below, shall be deemed to occur in the event that the following Service Levels are not met:

A. **Arbor Cloud Platform: 99.999% Availability**. The Arbor Cloud Platform, for purposes of the Arbor Cloud Services provided to End User, shall not be unavailable for more than twenty-six (26) consecutive seconds in any calendar month. For purposes of this Service Level, the term "available" means that the Arbor Cloud Service is available to the End User for use and is capable of receiving and routing network traffic via pre-provisioned GRE tunnels and/or DNS proxy only. Direct Connects are not part of the platform availability SLA.

B. **Standard Setup: 72 Hours**. Standard Setup shall be performed within seventy-two (72) hours of the completion of the provisioning call and acceptance of configuration submission by Licensor.

C. **Standard Updates: 72 Hours**. Standard Updates shall be performed within seventy-two (72) hours of the completion of the provisioning call and acceptance of configuration submission by Licensor.

D. **Emergency Setup: 4 Hours**. (Only applies to DNS Based Services). Emergency Setup shall be performed within four (4) hours of acceptance of configuration submission by Licensor.

E. **Emergency Updates: 4 Hours**. Emergency Updates shall be performed within four (4) hours of acceptance of configuration submission by Licensor.

F. **Mitigation Incident Initiation: 15 Minutes.** A Mitigation Incident conference bridge shall be initiated with available Licensor staff within fifteen (15) minutes of an End User initiating a mitigation request by a phone call to the Licensor Customer Support.

G. **BGP Route Announcement: 5 Minutes.** For BGP Based services, Licensor shall announce the End User BGP route to the Internet within five (5) minutes of all parties agreeing to initiate a mitigation and the End User completing any necessary routing changes on their End User premise equipment.

H. **Auto-Mitigation Initiation: Sub 1 Minute**. Licensor shall announce the End User BGP route to the Internet within one (1) minute of receiving the BGP route announcement from Customer using a BGP route triggered mitigation, within one minute (1) of receiving a Cloud Signal from a previously agreed upon and correctly configured Arbor APS or Arbor AED device, or within one (1) minute of detecting an attack using flow monitoring when setup for auto-mitigation.

I. **Mitigation Effectiveness: 5 Minutes/15 Minutes**. Mitigation Effectiveness shall mean the cleaning of the traffic such that no more than five percent (5%) of dirty/malicious traffic shall be passed to End User Endpoint(s). Licensor shall achieve Mitigation Effectiveness within: (i) five (5) minutes for Layer 3 and Layer 4 attacks from the time traffic is redirected to Arbor Cloud Platform and Licensor has detected malicious traffic; and (ii) fifteen (15) minutes for Layer 7 attacks from the time traffic is redirected to Arbor Cloud Platform and Licensor has detected malicious traffic. Each attack vector change shall restart timing of Mitigation Effectiveness.

2.2 A Service Outage shall not be deemed to occur when the event is due to any of the following: (a) inaccurate and/or insufficient information or configuration information provided by End User or failure by End User to comply with the ACS Description, including providing Licensor with access to, and ensuring availability of, the Endpoints; (b) misuse of the Arbor Cloud Services by End User; (c) traffic redirection delays (e.g. DNS TTLs and BGP route propagation delays) or other delays caused by upstream internet providers, such delays being outside of Licensor's control; (d) non-performance of a responsibility or any other obligation set forth herein or other negligent or unlawful acts or failure to act by End User or its agents or suppliers; (e) network unavailability outside of End User Endpoint(s), failure to implement ACLs or other documented best practices); (f) lack of End User participation in DDoS mitigation efforts, including Licensor's inability to reach End User by phone or End User's lack of English-speaking representatives available to coordinate and communicate with Licensor during a DDoS attack; (g) an End User provisioning request is not accepted by Licensor; (h) acts of God or events of force majeure (as described in the Agreement); (i) scheduled or emergency maintenance; (j) suspension or termination of the Arbor Cloud Services by Licensor in accordance with the terms of the ACS Description; or (k) End User has not directed all End User traffic for the Endpoint to the Arbor Cloud Platform.

3. SCHEDULED MAINTENANCE

Licensor may perform maintenance on its systems at any time but will be limited to a maximum of six (6) hours of scheduled maintenance per scrubbing center during any calendar week. Scheduled Maintenance

may result in the End User's inability to access (a) client-side web-based and mobile user interfaces, or (b) APIs, or other End User accessible software. Licensor will maintain a standard maintenance window on Sunday beginning at 0400 AM Greenwich Mean Time (GMT), but may initiate an additional maintenance window at a time period that is communicated to the End User at least forty-eight (48) hours in advance. Additionally, Licensor may perform emergency maintenance for no more than four (4) hours once per month per scrubbing center with four (4) hours advanced notice. Notice of Scheduled Maintenance will be provided to End User's designated point of contact by email or by a notification in the Arbor Cloud web- based user interface. The Arbor Cloud Platform will continue to be available for mitigation during most Scheduled Maintenance unless otherwise communicated to the End User at least forty-eight (48) hours in advance.

4. REMEDIES FOR SERVICE OUTAGES

4.1 Licensor shall, in good faith, determine whether a Service Outage occurred based on Licensor's records and data. In the event of a Service Outage, the following Credits will apply (as illustrated in Schedule 1 attached hereto – SLA Credit Calculation Chart):

A. **Credit – SLA: Arbor Cloud Platform: 99.999% Availability.** For a Service Outage occurring with respect to the SLA provided in 2.1.A, if the Service Outage is greater than: twenty-six (26) seconds but less than or equal to five (5) minutes, one (1) Credit shall apply; greater than five (5) minutes but less than or equal to one (1) hour, five (5) Credits shall apply; greater than one (1) hour, ten (10) Credits shall apply. To make a claim under 2.1.A, End User must send to Licensor Customer Support proof that the platform was unavailable for mitigation.

B. **Credit – SLA: Standard Setup and Standard Updates: 72 Hours.** For any Service Outage occurring with respect to the SLAs provided in 2.1.B and 2.1.C, if the Service Outage is greater than one (1) day but less than or equal to seven (7) days, one (1) Credit per day of Service Outage shall apply; greater than seven (7) days, ten (10) Credits shall apply.

C. **Credit – SLA: Emergency Setup and Emergency Updates: 4 Hours.** For any Service Outage occurring with respect to the SLAs provided in 2.1.D and 2.1.E, if the Service Outage is greater than one (1) hour, one (1) Credit per hour of Service Outage shall apply, up to a maximum of ten (10) Credits.

D. **Credit – SLA: Mitigation Incident Initiation: 15 Minutes.** For any Service Outage occurring with respect to the SLAs provided in 2.1.F, if the Service Outage for Mitigation Incident Initiation is greater than: fifteen (15) minutes, but less than or equal to thirty (30) minutes, one (1) Credit shall apply; greater than thirty (30) minutes, but less than or equal to sixty (60) minutes, two (2) Credits shall apply; greater than sixty (60) minutes, but less than or equal to four (4) hours, five (5) Credits shall apply; greater than four (4) hours, ten (10) Credits shall apply.

E. **Credit – SLA: BGP Route Announcement: 5 Minutes.** For any Service Outage occurring with respect to the SLAs provided in 2.1.G, if the Service Outage for BGP Route Announcement is greater than five (5) minutes, but less than or equal to fifteen (15) minutes, one (1) Credit shall apply; greater than fifteen (15) minutes, but less than or equal to sixty (60) minutes, two (2) Credits shall apply; greater than sixty (60) minutes, but less than or equal to four (4) hours, five (5) Credits shall apply; greater than four (4) hours, ten (10) Credits shall apply.

F. **Credit – SLA: Auto-Mitigation Initiation: Sub 1 Minute**. For any Service Outage occurring with respect to the SLAs provided in 2.1.H, if the Service Outage for Auto-Mitigation Initiation is greater than one (1) minute, but less than or equal to two (2) minutes, one (1) Credit

shall apply; greater than two (2) minutes, but less than or equal to five (5) minutes, two (2) Credits shall apply; greater than five (5) minutes, but less than or equal to fifteen (15) minutes, five (5) Credits shall apply; greater than fifteen (15) minutes, ten (10) Credits shall apply.

G. **Credit – SLA: Mitigation Effectiveness: 5 Minutes/15 Minutes.** For any Service Outage occurring with respect to the SLAs provided in Sections **2.1.I. and F**:

(1) if the Service Outage for Layer 3/4 is greater than five (5) minutes, but less than or equal to fifteen (15) minutes, one (1) Credit shall apply; greater than fifteen (15) minutes, but less than or equal to sixty (60) minutes, two (2) Credits shall apply; greater than sixty (60) minutes, but less than or equal to four (4) hours, five (5) Credits shall apply; greater than four (4) hours, ten (10) Credits shall apply.

(2) if the Service Outage for Layer 7 is greater than fifteen (15) minutes, but less than or equal to thirty (30) minutes, one (1) Credit shall apply; greater than thirty (30) minutes, but less than or equal to sixty (60) minutes, two (2) Credits shall apply; greater than sixty (60) minutes, but less than or equal to four (4) hours, five (5) Credits shall apply; greater than four (4) hours, ten (10) Credits shall apply.

To make a claim under **Sections 2.1.I**, End User must submit a packet capture of the traffic to the affected Endpoint of at least an hour of duration; provided, however, if End User is unable to provide the required packet capture of the duration set forth in this sentence, then End User shall provide Licensor with reasonable evidence to enable Licensor to verify the claim.

4.2 In the event End User believes a Service Outage has occurred, End User will provide to Licensor all relevant details and documentation supporting End User's claims of a Service Outage. Any claims for a Credit must be made by End User within seven (7) days after the alleged Service Outage and will be made to Licensor's Customer Support organization in writing. Claims made more than seven (7) days after the event will not be eligible for any of the remedies described herein. Licensor will investigate the claim and will respond back to End User within ten (10) business days of receipt of the notification of a claim from End User, either (i) accepting End User's Service Outage claim, or (ii) with all relevant details and documentation supporting a dispute of End User's Service Outage claim, in which case the parties shall resolve any such dispute promptly in good faith. Notwithstanding anything to the contrary set forth herein, (i) End User may not accumulate more than fifteen (15) Credits in any calendar month, and (ii) End User will not be entitled to any Credits if End User is in breach of the ACS Description at the time of the occurrence of the event giving rise to the Credit until End User has cured the breach. In addition, End User will not be entitled to a Credit if the event giving rise to the Credit would not have occurred but for End User's breach of the ACS Description or misuse of the Arbor Cloud Platform or the Arbor Cloud Services. Credits obtained by End User shall have no cash value but will apply against Service Package Fees in future invoices; provided, however, that if the Credits accrue in the last month of the Term and End User does not renew the Services and is not in default under the terms of the ACS Description or the Agreement, Licensor shall provide such Credits to End User in the form of a check within thirty (30) days of the end of the Term. Licensor will reflect Credits on invoices issued one calendar month after the occurrence of the Service Outage. Credits shall only apply to Services provided pursuant to the Service Fee set forth in the Quotation and will not apply to any other Licensor Services or any other form of custom development services provided by Licensor. Credits that would be available but for any of the limitations set forth in this section will not be carried forward to future months. End User's sole and exclusive remedy, and Licensor's sole and exclusive liability, in the event Licensor fails to provide the Arbor Cloud Services in accordance with the ACS Description and this Service Level Agreement, shall be to receive a Credit in accordance with the terms of this **Section 4**.

SCHEDULE 1 TO SERVICE LEVEL AGREEMENT FOR ARBOR CLOUD SERVICE
SLA CREDIT CALCULATION CHART

Credit as described in Section 4.1A ***Service Outage for SLA provided in Section 2.1A (Arbor Cloud Platform)***		
Service Outage Greater Than	**Service Outage Less than or Equal to**	**Amount of Credit**
26 seconds	5 minutes	1 Credit
5 minutes	1 hour	5 Credits
1 hour		10 Credits

Credit as described in Section 4.1B ***Service Outage for SLA provided in Section 2.1B (Standard Setup) and 2.1C (Standard Updates)***		
Service Outage Greater Than	**Service Outage Less than or Equal to**	**Amount of Credit**
1 day	7 days	1 Credit per day of Service Outage
7 days		10 Credits

Credit as described in Section 4.1C ***Service Outage for SLA provided in Section 2.1D (Emergency Setup) and 2.1E (Emergency Updates)***		
Service Outage Greater Than	**Service Outage Less than or Equal to**	**Amount of Credit**
1 hour		1 Credit per hour of Service Outage, up to a maximum of 10 Credits

Credit as described in Section 4.1D ***Service Outage for SLA provided in Section 2.1F (Mitigation Incident Initiation)***		
Service Outage Greater Than	**Service Outage Less than or Equal to**	**Amount of Credit**
15 minutes	30 minutes	1 Credit
30 minutes	60 minutes	2 Credits
60 minutes	4 hours	5 Credits
4 hours		10 Credits

Credit as described in Section 4.1E ***Service Outage for SLA provided in Section 2.1G (BGP Route Announcement)***		
Service Outage Greater Than	**Service Outage Less than or Equal to**	**Amount of Credit**
5 minutes	15 minutes	1 Credit
15 minutes	60 minutes	2 Credits
60 minutes	4 hours	5 Credits
4 hours		10 Credits

Credit as described in Section 4.1F *Service Outage for SLA provided in Section 2.2H (Auto-Mitigation Initiation)*		
Service Outage Greater Than	**Service Outage Less than or Equal to**	**Amount of Credit**
1 minute	2 minutes	1 Credit
2_ minutes	5 minutes	2 Credits
5_ minutes	15 minutes	5 Credits
15 minutes		10 Credits

Credit as described in Section 4.1G(1) *Service Outage for SLA provided in Section 2.2I for Layer 3 & 4 attacks (Mitigation Effectiveness)*		
Service Outage Greater Than	**Service Outage Less than or Equal to**	**Amount of Credit**
5 minutes	15 minutes	1 Credit
15 minutes	60 minutes	2 Credits
60 minutes	4 hours	5 Credits
4 hours		10 Credits

Credit as described in Section 4.1G(2) *Service Outage for SLA provided in Section 2.2I for Layer 7 attacks (Mitigation Effectiveness)*		
Service Outage Greater Than	**Service Outage Less than or Equal to**	**Amount of Credit**
15 minutes	30 minutes	1 Credit
30 minutes	60 minutes	2 Credits
60 minutes	4 hours	5 Credits
4 hours		10 Credits

Příloha č. 4: Seznam členů realizačního týmu

Seznam členů realizačního týmu

Poř. číslo	Jméno	Příjmení	Role	č. MT	Email	Dny dosahu	Hodiny dosahu
1	[redacted]						
2							
3							
Případní náhradníci							