evid. č. u Poskytovatele: RCJ-250099
evid. č. u Objednatele: 9730/00135

SMLOUVA O SLUŽBÁCH

uzavřená v souladu s § 1746 odst. 2. zákona č. 89/2012 Sb., občanský zákoník
(dále jen „**smlouva**“)

Článek I.
Smluvní strany

Veterinární univerzita Brno
Sídlo: Palackého tř. 1, 612 42 Brno
IČO: 62157124
DIČ: CZ62157124
Zastoupené: Ing. Bc. Radko Bébarem, kvestorem VETUNI

Kontaktní osoba: xxx
E-mail: xxx@VFU.cz

(dále jen „Objednatel“)

a

Aricoma Systems a.s
Sídlo *(místo podnikání)*: Hornopolní 3322/34, Moravská Ostrava, 702 00 Ostrava
doručovací adresa: Sochorova 23, 616 00 Brno
Zastoupená*(ý)*: **Petrem Konečným, ředitel RC, na základě plné moci**
IČ: 04308697
DIČ: CZ04308697
Bankovní spojení: Česká spořitelna a.s.
Číslo účtu: 6563752/0800
(dále jen „Poskytovatel“)

Článek II.
Předmět smlouvy

1. Touto smlouvou se Poskytovatel zavazuje vlastním jménem a na vlastní odpovědnost poskytovat Objednateli odborné služby specifikované v čl. III. smlouvy a Objednatel se zavazuje za tyto odborné služby zaplatit cenu sjednanou podle čl. VI. této smlouvy.

Poskytovatel prohlašuje, že má dostatečné odborné kapacity ke splnění závazků z této smlouvy.

2. Nedílnou součástí této smlouvy je Příloha č. 1. - Kybernetická opatření.

Článek III.

Specifikace plnění

1. Předmětem plnění podle této smlouvy je soubor služeb a aktivit spojený s digitální transformací VETUNI v oblasti zvýšení kyberbezpečnosti prostřednictvím zajištění pokročilé správy koncových zařízení, prostřednictvím software Microsoft 365 Intune. Plnění Poskytovatele zahrnuje zejména analýzu stávajícího IT prostředí Objednatele a návrh implementace Microsoft 365 Intune, nasazení a konfiguraci Intune, testování a vyladění služeb podle potřeb Objednatele tak, jak jej stanoví Kontaktní osoba, skolení zaměstnanců na správu systému a využití řešení, a poskytnutí veškeré potřebné dokumentace.

2. Poskytovatel provede administrátory Objednatele návrhem, konfigurací, nasazením a optimalizaci řešení, které umožní centralizovanou správu koncových zařízení, automatizaci procesů a zvýšení ochrany univerzitních dat v prostředí M365 Intune. Dále je součástí Poskytovatelova plnění proškolení příslušných zaměstnanců pro efektivní využívání systému a zajištění kvalitní technické podpory. Implementací tohoto řešení dojde k optimalizaci IT procesů, minimalizaci provozních rizik a posílení kybernetické bezpečnosti univerzity.
3. Poskytovatel prohlašuje, že jím stanovená osoba pro plnění služby má potřebné zkušenosti s implementací Microsoft 365 Intune a integrací Intune do firemního IT prostředí. Poskytovatel rovněž prohlašuje, že je má certifikaci Microsoft Partner nebo obdobnou odbornou kvalifikaci dosvědčující jeho odbornost, a že je schopen zaměstnancům Objednatele poskytovat potřebné školení a technickou podporu.

4. Poskytovatel neodpovídá za obsah již zpracovaných dokumentů Objednatele, které mu Objednatel předá v rámci realizace předmětu plnění, ale odpovídá výhradně za dokumentaci vzniklou v rámci průběhu plnění předmětu smlouvy.

Článek IV.

Termíny a místo plnění

1. Smluvní strany se dohodly na zahájení plnění podle této smlouvy v termínu od účinnosti této smlouvy. Jednotlivá plnění a služby budou poskytována dle požadavků Objednatele ve stanovených termínech.

2. Místo poskytování odborných služeb a místo předání plnění je sídlo Objednatele a sídlo Poskytovatele, nedohodnou-li se strany jinak. Smluvní strany souhlasí s využitím nástrojů elektronické komunikace a online schůzek, bude-li to efektivní s ohledem na agendu. Spočívá-li plnění v osobní účasti Poskytovatele na jednání dle požadavku Objednatele, je místem plnění místo jednání určené Objednatelem.

Článek V.

Způsob plnění

1. Služby podle této smlouvy budou prováděny Poskytovatelem průběžně po dobu trvání smlouvy v rozsahu specifikovaném v článku III. této smlouvy a dále podle požadavků Objednatele.
2. V případě, že Objednatel bude požadovat poskytnutí služby formou účasti Poskytovatele na jednání pracovní skupiny Objednatele, zavazuje se Objednatel oznámit nejpozději 5 pracovní dny dopředu termín a místo konání pracovního jednání včetně programu tohoto jednání na kontaktní e-mail Poskytovatele.
3. Výstupy specifikované v článku III, zpracované Poskytovatelem písemně, budou předány Poskytovatelem v elektronické formě. Elektronickou formu plnění lze Objednateli předat na kontaktní e-mailovou adresu Objednatele, uvedenou v čl. I smlouvy.
4. Veškerá jednání a korespondence budou probíhat v českém jazyce.

Článek VI.

Cena a platební podmínky

1. Služby budou poskytovány za člověkohodinovou sazbu, která činí xxxxx Kč bez DPH, DPH 21 % činí xxx Kč, tj. celkem xxx DPH.
2. Maximální rozsah poskytnutých služeb je shora omezen částkou 300 000 Kč bez DPH.
3. Sjednaná cena za hodinu poskytování Služby dle odst. VI.1 Smlouvy je cena konečná a nepřekročitelná zahrnujícími veškeré náklady Poskytovatele související s poskytováním Služby.
4. Při výpočtu úhrady za Služby dle čl. III. se bude vycházet ze skutečného rozsahu, tj. Poskytovatelem odpracovaného počtu hodin pro Objednatele.
5. Písemné odsouhlasení výkazu skutečného rozsahu poskytnutých Služeb Kontaktní osobou Objednatele, je nutnou podmínkou pro vznik práva Poskytovatele na vystavení daňového dokladu (faktury).

6. Cenu za poskytnutou Službu bude Objednatel hradit měsíčně zpětně na základě faktury vystavené Poskytovatelem. Přílohou faktury bude vždy příslušný, kontaktní osobou Objednatele odsouhlasený, výkaz.
7. Faktura musí obsahovat náležitosti daňového dokladu předepsané příslušnými právními předpisy (zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů), odkaz na evidenční číslo smlouvy a dále vyčíslení zvlášť ceny bez DPH, zvlášť DPH a celkovou cenu včetně DPH.
8. Smluvní strany se dohodly na bezhotovostní úhradě ceny a lhůtě splatnosti v délce 14 kalendářních dnů ode dne doručení faktury Objednateli.
9. Poskytovatel je povinen vystavit a Objednateli předat daňový doklad v elektronickém formátu IS DOC/IS DOCx, nebo ve formátu PDF, a to prostřednictvím datové schránky (y2cj9e8) nebo na email: zurekl@vfu.cz. Případné přílohy faktury, které jsou považovány za nezbytnou náležitost faktury, mohou být připojeny v souboru .ZIP nebo .RAR v pořadí – 1. faktura jako hlavní dokument, 2. přílohy k faktuře jako příloha dokumentu.

Článek VII.

Mlčenlivost

1. Poskytovatel se zavazuje po dobu trvání smluvního vztahu založeného touto smlouvou i po jeho skončení vůči třetím osobám zachovávat mlčenlivost o všech informacích, které se dozvěděl v souvislosti s realizací plnění dle této smlouvy a nesmí je zpřístupnit bez písemného souhlasu Objednatele žádné třetí osobě ani je použít v rozporu s účelem této smlouvy, ledaže se jedná:
   a) o informace, které jsou veřejně přístupné, nebo
   b) o případ, kdy je zpřístupnění informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu.
2. Poskytovatel je povinen zavázat povinností mlčenlivosti podle odstavce 1. všechny osoby, které se budou podílet na plnění podle této smlouvy.
3. Za porušení povinnosti mlčenlivosti osobami, které se budou podílet na poskytování služeb dle této smlouvy, odpovídá Poskytovatel, jako by povinnost porušil sám.
4. Povinnost zachovat mlčenlivost trvá i po skončení účinnosti této smlouvy.
5. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím osob oprávněných jednat jménem smluvních stran, kontaktních osob, popř. jimi pověřených pracovníků.

6. Článek IX.

Závěrečná ustanovení

1. Žádná ze smluvních stran není odpovědná za neplnění závazku způsobené okolnostmi nezávislými na její vůli (vyšší mocí). Příkladem takových okolností jsou např. stávky, teroristické útoky, válka, problémy v zásobování, přepravě či výrobě, změny kurzu, vládní či regulační opatření a přírodní katastrofy. Kterákoliv smluvní strana je oprávněna v takovém případě plnit svůj závazek v přiměřeně prodloužené lhůtě.
2. Tato Smlouva a veškeré otázky s ní související, jakožto i otázky platnosti smlouvy, se řídí český právem.
3. Tato smlouva je sepsána ve dvou vyhotoveních s platností originálu, z nichž obě smluvní strany obdrží po jednom. Smlouvu lze podepsat elektronicky oběma stranami a pak stačí jen jeden exemplář sdílený elektronicky.
4. Smlouva nabývá platnosti dnem podpisu smluvními stranami a účinnosti dnem zveřejnění smlouvy dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) a její platnost končí dne 31. prosince 2024. Poskytovatel podpisem této smlouvy souhlasí s jejím uveřejněním v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, a to v plném rozsahu.
5. Tuto smlouvu lze měnit jen formou písemných dodatků podepsaných oběma smluvními stranami.
6. Smluvní strany prohlašují, že si tuto Smlouvu pozorně přečetly a že je jim její obsah jasný a srozumitelný. Na důkaz toho, že celý obsah Smlouvy je projevem jejich pravé a svobodné vůle, připojují Smluvní strany své podpisy.

V Brně dne

Za Objednatele:

Za Poskytovatele:

_____

Veterinární univerzita Brno
Ing. Bc. Radko Bébar, kvestor VETUNI

_____

Aricoma Systems a.s.
Petr Konečný

Příloha č. 1 - Kybernetická opatření

1. Systém řízení bezpečnosti informací

1.1 Poskytovatel bere na vědomí, že VETUNI má zaveden systém řízení bezpečnosti a je osobou dle § 3 odst. e) Zákona o kybernetické bezpečnosti a je povinen naplnit požadavky související legislativy.

1.2 Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření VETUNI.

1.3 Poskytovatel se zavazuje:

a) Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění.

b) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.

c) Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.

d) Vytvořit a schválit bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.

e) Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

f) Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy VETUNI zpřístupnit.

g) Využívá-li při poskytování předmětu plnění poddodavatele, zajistit adekvátní dodržování těchto Bezpečnostních požadavků rovněž ve smluvních vztazích se svými poddodavateli.

h) Po skončení plnění smlouvy bez zbytečného odkladu skartovat veškeré informace a data VETUNI, které mu byly v souvislosti s plněním smlouvy předány.

2. Bezpečnost lidských zdrojů

2.1 Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na dodržování, provozu a rozvoji bezpečnostních opatření VETUNI a zároveň se zavazuje:

a) Zajistit, aby Odpovědná osoba ve věcech smluvních nejpozději do 10 dnů od uzavření smlouvy potvrdila písemně VETUNI, že všechny osoby podílející se na poskytování předmětu plnění za stranu Poskytovatele byly prokazatelně seznámeny s těmito Bezpečnostními požadavky a s pravidly kybernetické bezpečnosti VETUNI.

b) Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny s těmito pravidly a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

c) Dodržovat příslušná ustanovení vnitřních norem a předpisů VETUNI v rozsahu, v jakém byl s těmito akty prokazatelně seznámen. Za prokazatelné seznámení se považuje protokolární či elektronické předání příslušné dokumentace nebo VETUNI zajištěný přístup na sdílené úložiště obsahující příslušné interní řídící akty.

d) V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.
e) Zajistit, aby osoby podílející se na poskytování plnění VETUNI v prostředí nebo s prostředky VETUNI, a to i tehdy, pokud jsou prostředky VETUNI používány mimo jeho prostředí:
- Pro uložení a sdíleni dat a informací VETUNI využívaly pouze k tomu schválené prostředky;
- Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno VETUNI;
- Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;
- Nenavštěvovaly internetové stránky s eticky či zákonně nevhodným obsahem;
- Nerealizovaly pokusy o neautorizovaný přístup ke zdrojům VETUNI ani ke zdrojům jiných subjektů;
- Nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků VETUNI, a to ani v případě, kdy jim byl prostředek VETUNI svěřen do správy;
- Nepodílely se s prostředky VETUNI na šíření spamu ani škodlivého softwaru.
2.2 Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům VETUNI je na straně VETUNI zpracování osobních údajů pracovníků Poskytovatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude VETUNI umožněno osobní údaje dotčených pracovníků Poskytovatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům VETUNI.
3. Řízení provozu a komunikací
3.1 Poskytovatel se zavazuje:
a) Zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.
b) Na vyžádání poskytnout VETUNI přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře, pokud je ta používána v souvislosti s předmětem plnění.
c) Zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění a práva třetích osob.
4. Řízení přístupu a bezpečné chování uživatelů
4.1 Poskytovatel se zavazuje:
a) Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům VETUNI.
b) Zajistit, aby udělený přístup nebyl sdílen více osobami za stranu Poskytovatele.
c) Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k IT systému VETUNI požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).
d) Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivum VETUNI chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

e) Průběžně kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do prostředí VETUNI.
4.2 Poskytovatel bere na vědomí, že přístup k systému IT je možné povolit pouze fyzické identitě zaměstnance poskytovatele / poddodavatele poskytovatele s vygenerovaným jednoznačným identifikátorem, a to na základě požadavku poskytovatele na přístup. Pro vytvoření identifikátoru je nezbytné sdělení těchto osobních údajů zaměstnance Poskytovatele:
- Jméno
- Příjmení
- Datum narození
- Rodné číslo (ŘČ v systémech neukládáme, nepožadujeme jeho zasílání ani zaznamenání do formuláře ale je vyžadováno při generování identifikátoru IPD, kdy toto fyzická identita sdělí v okamžiku generování jednoznačného identifikátoru IPD. V případě nesouhlasu fyzické osoby s použitím RČ je IPD generováno z data narození a dalších osobních údajů fyzické osoby).
- Email
- Mobilní telefon případně pevná linka
4.3 Poskytovatel se zavazuje informovat své zaměstnance a poddodavatele, kterým bude přidělen přístup (fyzický, logický) k systému IT, o způsobu zpracování jejich osobních údajů a VETUNI se zavazuje zpracovávat osobní údaje výhradně v souladu s platným právním řádem (GDPR).
4.4 Poskytovatel bere na vědomí, že přidělení oprávnění zaměstnanci poskytovatele bude řízeno principem nezbytného minima a není nárokové.
4.5 Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Poskytovatele) 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).
5. Akvizice, vývoj a údržba
5.1 Poskytovatel se zavazuje:
a) Zajistit bezpečnou implementaci, inovaci, aktualizaci, a testování technologií, které jsou předmětem plnění.
b) Předat VETUNI dokumentaci předmětu plnění minimálně v následujícím rozsahu:
- dokumentaci skutečného provedení
- dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů
- dokumentaci obsahující popis autorizačního konceptu a oprávnění
- dokumentaci obsahující zálohovací a archivační postupy
- dokumentaci obsahující instalační a konfigurační postupy
- dokumentaci pro zajištění kontinuity provozu a obnovy po havárii
5.2 V případě, že předmět plnění zahrnuje vývoj softwaru, zavazuje se Poskytovatel:
a) Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu.
b) Pokud jsou softwarové auditní činnosti a předání zdrojového kódu k software součástí plnění dle Smlouvy, umožní Poskytovatel VETUNI audit prováděného nebo provedeného plnění a na písemnou žádost VETUNI předloží Poskytovatel VETUNI vyvíjený zdrojový kód k

software na provedení codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), a to zejména za účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu se Smlouvou a těmito Bezpečnostními požadavky.
c) Poskytovat VETUNI v termínech stanovených VETUNI, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání.
d) Zajistit, že plnění bude 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, bloatware apod.).
e) 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 VETUNI.
f) Zajistit bezpečnost testovacího prostředí u Poskytovatele a ochranu poskytnutých testovacích dat VETUNI.
g) Zajistit, že v produkčním prostředí VETUNI bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění.
h) Zajistit, že v rámci poskytovaného plnění bude dodávaný software
- v souladu s bezpečnostními politikami a standardy VETUNI
- otestován na soulad s bezpečnostními politikami VETUNI (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami seznámen)
i) Instalovat software pouze na základě VETUNI předem schválených migračních postupů.
j) Předat zdrojový kód VETUNI bezpečnou formou zajišťující jeho integritu.
k) Zajistit řízení verzí zdrojového kódu.
l) Zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.
m) Zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů.
n) Nevyvíjet, nekompilovat a nešířit v prostředí VETUNI programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.
6. Zvládání kybernetických bezpečnostních událostí a incidentů
6.1 Poskytovatel se zavazuje:
a) Bez zbytečného odkladu hlásit VETUNI všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na VETUNI, a to způsobem stanoveným ve smlouvě.
b) Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.
c) V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout VETUNI součinnost a relevantní informace o podezřelém zařízení na straně Poskytovatele.

d) Bez zbytečného odkladu a po dohodě s VETUNI realizovat opatření, požadovaná VETUNI v dohodnutých termínech, ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu, který může mít dopad na VETUNI.
e) Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že poskytovatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
6.2 Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Bezpečnostních požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující odpovědnost poskytovatele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy poskytovateli či jiné osobě ze strany VETUNI. Ostatní ustanovení ohledně odpovědnosti poskytovatele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.
7. Řízení kontinuity činností
7.1 Poskytovatel se zavazuje:
a) Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
b) Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně služeb.
8. Fyzická bezpečnost
8.1 Poskytovatel se zavazuje:
a) Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů IT, anebo datové nosiče.
b) V rozsahu předmětu plnění zajistit fyzické zabezpečení instalačních, záložních nebo archivních médií a dokumentace v souladu se zákonem, zejména označení, uchování a likvidaci.
9. Bezpečnostní nástroje
9. 1. Poskytovatel se zavazuje:
a) Realizovat bezpečnostní opatření pro odstranění nebo blokování síťových spojení, která neodpovídají požadavkům na ochranu integrity komunikační sítě.
b) Realizovat přístup z mobilního zařízení do prostředí VETUNI pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN).
c) Připojovat do prostředí VETUNI pouze ta zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně VETUNI určenou ve smlouvě.
d) Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Poskytovatele.
e) Na aktiva VETUNI neinstalovat a nepoužívat v prostředí VETUNI tyto typy nástrojů, pokud nejsou výslovně součástí předmětu plnění:
- Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
- Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

- Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů IT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.
- Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému IT.
- Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí VETUNI.

f) Připojovat do prostředí VETUNI pouze zařízení IT, která splňují tyto požadavky:
- musí být aplikovány bezpečnostní záplaty (operačního systému, internetového prohlížeče a dále balíku MS Office, Javy a případně dalšího software vybavení, pokud je používáno);
- musí mít nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.
- Používaná paměťová média (flash disky, CD a DVD, apod.), musí být před použitím zkontrolována v zařízení, které má nainstalovanou aktualizovanou antivirovou ochranu.
- Musí být připojováno pouze do vyhrazené bezpečnostní zóny a způsobem definovaným v provozní nebo projektové dokumentaci. Pokud v provozní nebo projektové dokumentaci definováno není, předpokládá se, že se připojení takových zařízení nedovoluje.

g) Průběžně zaznamenávat a uchovávat data o provozu zařízení IT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy.
h) Na vyžádání poskytnout VETUNI report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.
i) Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.
j) Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.
k) Veškeré neveřejné informace poskytnuté VETUNI chránit vhodným šifrováním a proti neautorizovanému přístup, a to zejména na mobilních zařízeních.

9.2 Poskytovatel bere na vědomí, že v případě, kdy technické spojení společnosti VETUNI s Poskytovatelem narušuje chod VETUNI, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud smlouva nestanoví jinak.
9.3 Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí VETUNI jsou monitorovány a vyhodnocovány v rozsahu předměty plnění a v souladu s interními dokumenty VETUNI, se kterými byl Poskytovatel seznámen.