Příloha č. 9

Bezpečnostní požadavky

A. Kybernetické požadavky

Za účelem naplnění povinností stanovených Objednateli, jakožto povinné osobě dle ZKB a VKB, je Poskytovatel povinen, nad rámec povinností stanovených v jiných částech Smlouvy plnit níže uvedené povinnosti zejména součinnostního a bezpečnostního charakteru (dále také jen „*Kybernetické požadavky*").

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

1. Systém řízení bezpečnosti informací

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 3 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění na své straně:
    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. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
    c. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.
    d. Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně 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. Poskytovatel je dále povinen dodržovat bezpečnostní politiku Objednatele, byl-li s ní seznámen.

2. Řízení aktiv

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 4 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění (aktivy se rozumí např. data a informace k předmětu plnění, systémy ICT, moduly, hardware prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli předložit do třiceti (30) dnů od nabytí účinnosti Smlouvy a následně na vyžádání, a to po celou dobu trvání smluvního vztahu a po dobu dvou (2) let po jeho ukončení.

3. Řízení rizik

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 5 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
   b. V minimálním intervalu 1x ročně vytvořit a předložit Objednateli zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
      i. Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;
      ii. Identifikaci a hodnocení rizik s vazbou na předmět plnění;
      iii. Realizovaná bezpečnostní opatření;
      iv. Nepokrytá bezpečnostní rizika a návrh opatření;
      v. Vyhodnocení bezpečnostních událostí a incidentů; a
      vi. Aktuální stav souladu Poskytovatele s Kybernetickými požadavky.

4. Organizační bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 6 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. Do 30 dnů od nabytí účinnosti smluvního vztahu jmenovat odpovědnou kontaktní osobu pro kybernetickou bezpečnost pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi smluvními stranami.
   b. Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny s příslušnými Interními předpisy Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

5. Řízení poddodavatelů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Využívá-li při poskytování předmětu plnění poddodavatele, zabezpečit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Poskytovatel zavazuje doložit Objednateli do deseti (30) dnů od nabytí účinnosti Smlouvy, a dále vždy v případě změny poddodavatele, a to písemným prohlášením Poskytovatele o dodržování Kybernetických požadavků u svých poddodavatelů.
    b. Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zabezpečit nad rámec odst. 18.3 Smlouvy uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění) ve smyslu příslušných ustanovení nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

6. Bezpečnost lidských zdrojů

1. Poskytovatel se bude v rozsahu předmětu aktivně podílet na splnění povinností uvedených v § 9 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. zabezpečit, aby Kontaktní osoba pro kybernetickou bezpečnost nejpozději do třiceti (30) dnů od účinnosti Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění Smlouvy za Poskytovatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních předpisů Objednatele.
    b. Přiměřeně dodržovat příslušná ustanovení interních předpisů Objednatele v rozsahu, v jakém byl s těmito předpisy seznámen. Za prokazatelné seznámení se považuje školení pracovníků Poskytovatele zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní předpisy.
    c. 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.
    d. Zabezpečit, aby osoby podílející se na poskytování předmětu plnění v IT prostředí objednatele anebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo IT prostředí objednatele:
        i. Pro uložení a sdíleni dat a informací Objednatele využívali pouze k tomu schválené prostředky (aktiva) a schválené způsoby komunikace;
        ii. Neukládali ani nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;

iii. Nestahovali, nesdíleli, neukládali, nearchivovali ani neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo předpisy upravující ochranu duševního vlastnictví;

iv. Nenavštěvovali internetové stránky s eticky nevhodným obsahem;

v. Nerealizovali pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů; a

vi. Nerealizovali pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;

vii. Nepodíleli se s prostředky Objednatele na šíření spamu ani škodlivého softwaru;

viii. Dodržovali obecně závazné právní předpisy.

2. Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je zpracování osobních údajů pověřených osob Poskytovatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Objednateli umožněno osobní údaje dotčených pověřených osob Poskytovatele zpracovat, nebude těmto pověřeným osobám umožněn žádný přístup ke zdrojům Objednatele.

7. Řízení provozu a komunikací

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 10 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

   a. Zabezpečit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění.

   b. Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

   c. Zabezpečit, 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 licenční podmínky a předpisy upravující ochranu duševního vlastnictví.

8. Řízení změn

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 11 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

   a. Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.

   b. Aktivně spolupracovat při testování významné změny.

9. Řízení přístupu

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 12 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Přidělovat oprávnění svým jednotlivým pověřeným osobám ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.
    b. Zabezpečit, aby udělený přístup nebyl sdílen více osobami Poskytovatele, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Poskytovatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání tohoto smluvního vztahu a dva (2) roky po jeho ukončení.
    c. Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k IT prostředí objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).
    d. Zabezpečit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům Objednatele (IT prostředí Objednatele) chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.
    e. Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do IT prostředí Objednatele.
2. Poskytovatel bere na vědomí, že přístup k IT prostředí Objednatele je možné povolit pouze fyzické identitě zaměstnance Poskytovatele / poddodavatele Poskytovatele, a to na základě požadavku Poskytovatele na přístup těchto osob.
3. Poskytovatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.
4. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby na straně 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 Objednatele).

10. Akvizice, vývoj a údržba

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 13 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
    a. Zabezpečit bezpečnou implementaci, inovaci, aktualizaci a testování technologií v případě, že jsou předmětem plnění, ledaže tyto činnosti provádí Objednatel.
    b. Předat Objednateli v přiměřené lhůtě stanovené Objednatelem dokumentaci předmětu plnění minimálně v následujícím rozsahu:

i. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;

ii. dokumentaci obsahující popis autorizačního konceptu a oprávnění;

iii. dokumentaci obsahující instalační a konfigurační postupy.

2. V případě, že předmět plnění zahrnuje vývoj softwaru, zavazuje se Poskytovatel:

   a. Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru v závislosti na charakteru plnění.

   b. Na vyžádání umožnit Objednateli provedení auditu prováděného nebo provedeného plnění, předložit Objednateli vyvíjený zdrojový kód na provedení codereview anebo výstupy z provedeného codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně) po jeho dokončení, pokud není ve Smlouvě stanoveno jinak, a to zejména za účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu s ustanoveními tohoto smluvního vztahu a těmito Kybernetickými požadavky.

   c. Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání.

   d. Zabezpečit, že předmět plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru anebo které jsou specifikovány výslovně v této Smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

   e. Pokud je součástí předmětu plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí Objednatele.

   f. Zabezpečit bezpečnost testovacího prostředí u Poskytovatele (pokud testovací prostředí neprovozuje Objednatel) a ochranu poskytnutých testovacích dat Objednatelem.

   g. Zabezpečit, že do produkčního prostředí Objednatele bude dodán jen smluvně specifikovaný kompilovaný, respektive spustitelný zdrojový kód a další nezbytná data pro provozování předmětu plnění.

   h. Zabezpečit, že v rámci poskytovaného předmětu plnění bude dodávaný software:

      i. v souladu s bezpečnostními politikami a standardy Objednatele (Interními předpisy); a

      ii. otestován na soulad s bezpečnostními politikami Objednatele (platí pro Poskytovatele, pokud byl s takovými bezpečnostními politikami (Interními předpisy) seznámen).

i. Instalovat software pouze na základě Objednatelem předem schválených migračních postupů.

j. Předat zdrojový kód Objednateli bezpečnou formou zajišťující jeho integritu.

k. Zabezpečit řízení verzí zdrojového kódu.

l. Zabezpečit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.

m. Zabezpečit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů.

n. Nevyvíjet, nekompilovat a nešířit v prostředí Objednatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

11. Zvládání kybernetických bezpečnostních událostí a incidentů

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 14 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

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

   b. Bez zbytečného odkladu hlásit Objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na Objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby pro kybernetickou bezpečnost.

   c. Vyhodnocovat ve svém prostředí a v rozsahu odpovídajícímu předmětu plnění informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

   d. V případě vzniku bezpečnostní události, která může mít potenciálně dopad na předmět plnění či jinak ohrozit nebo omezit Objednatele, a následného zvládání a vyhodnocování bezpečnostního incidentu anebo v případě podezření na bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Poskytovatele.

   e. Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.

   f. Spolupracovat při analýze příčin bezpečnostního incidentu, na vyžádání poskytnout Objednateli všechny podklady (logy, záznamy apod.) a navrhnout opatření s cílem zamezit jeho opakování v případě.

2. Objednatel může s cílem identifikovat bezpečnostní incidenty zaznamenávat, a to jakýmkoli způsobem a bez časového omezení, všechny činnosti, které Poskytovatel realizuje v prostředí Objednatele.

3. Poskytoval je povinen zajistit aktivní součinnost svých pracovníků při vyšetřování bezpečnostních incidentů, a to i těch, které mohla způsobit jiná osoba než Poskytovatel.
4. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující povinnost k náhradě újmy Poskytovatele za prodlení s řádným a včasným plněním předmětu plnění a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele. Ostatní smluvní ustanovení ohledně odpovědnosti Poskytovatele za prodlení nejsou tímto ustanovením dotčena.

12. Řízení kontinuity činností

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 15 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel 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.

13. Kontrola a audit

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 8 a § 16 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany NÚKIB dle § 23 ZKB.

14. Fyzická bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 17 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče (Interní předpisy).
   b. V rozsahu předmětu plnění zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv Objednatele, pokud s ní byl Poskytovatel seznámen.

15. Bezpečnostní nástroje

1. Poskytovatel se bude v rozsahu předmětu plnění aktivně podílet na splnění povinností uvedených v § 18 až § 27 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:

a. Realizovat bezpečnostní opatření pro odstranění anebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.

b. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím šifrovaného připojení, využívat virtuální privátní síť (VPN), pokud takový ji Objednatel Poskytovateli zajistil, nebo zvolit adekvátní technické opatření k ochraně informací.

c. Pokud je to předmětem plnění, připojovat do IT prostředí Objednatele pouze taková síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele.

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 Objednatele neinstalovat a nepoužívat v IT prostředí objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:

    i. Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

    ii. Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

    iii. Analyzátor zranitelností (scanner zranitelností) – softwarový anebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.

    iv. Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.

    v. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.

f. Připojovat do IT prostředí objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.

g. Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné a účinné české a evropské legislativy.

h. Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu

předmětu plnění, a to po celou dobu trvání smluvního vztahu a po dobu dvou (2) let po jeho ukončení.

i. Zabezpečit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením anebo 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 Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

2. Poskytovatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Poskytovatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění.

B. Minimální bezpečnostní standard GAČR

Požadavky na zapojení a provoz počítačů/zařízení v datové síti Objednatele (dále také jen „*GA ČR*"), týká se počítačů/zařízení připojených do interní sítě GA ČR.

GA ČR je dle ZKB určena coby správce a provozovatel několika významných informačních systémů.

Instalační standardy kyberbezpečnosti GA ČR:

a) Počítače musí být s operačním systémem min. Microsoft Windows 10 Professional CZ a vyšší (Windows 10 Home jsou nepřípustné) a jsou součástí domény Microsoft Active Directory gacr.cz

b) Na koncových stanicích Windows musí mít uživatel práva pouze jako user. Uživatelé musí být autorizováni proti Microsoft Active Directory.

c) Uživatel musí být autorizován loginem a heslem (nepřipouští se jeden anonymní účet pro všechny uživatele). Každý zaměstnanec GA ČR má přidělen jeden unikátní login.

d) Na počítači/zařízení musí být instalován antivirový program GA ČR s centrální správou. Aktuální antivirový program používaný v GA ČR je ESET.

e) Systémové služby aplikace musí být spouštěny na pozadí bez nutnosti spouštět je pod přihlášeným uživatelem.

f) Share adresáře jsou centrální a jsou tedy upřednostňovány. Výjimky je nutno žádat na oddělení IT (OITPaR) GA ČR.

g) Jakékoliv vystavené služby nebo zdroje v datové síti GA ČR musí být autorizovány loginem a heslem proti Microsoft Active Directory gacr.cz.

h) Veškeré webové služby musí být realizovány jako SSL. Certifikáty poskytuje OITPaR GA ČR.

i) Čas se synchronizuje z NTP serverů CESNET.

j) Počítač/zařízení musí mít instalovaného klienta desktop managementu, kterým je plošně zajišťována aktualizace operačního systému a instalovaných aplikací. Aktualizační balíčky aplikací si zajišťuje dodavatel aplikace na vlastní náklady.

k) Pro serverová zařízení je vyžadováno umožnění zapojení do monitoringu Paesler PRTG monitor a Lansweeper

l) Administrátorské heslo musí odpovídat bezpečnostním standardům GA ČR, délka minimálně 17 míst, velká a malá písmena, čísla, speciální znaky, změna hesla minimálně 1x za 18 měsíců

m) Systém musí logovat veškeré činnosti uživatelů a administrátorů tak, aby bylo možné zpětně identifikovat provedené změny a jejich původce.

n) Pro identifikaci v datové síti bude lokální firewall umožňovat minimálně ICMP ECHO (ping)

o) Veškeré SW příslušenství, které tvoří nedílnou součást předmětu plnění (např. operační systém, který tvoří nedílnou součást dodávaného zařízení, ovládací SW atd.), musí být v poslední (nejnovější) verzi, kterou výrobce SW k datu podání nabídky nabízí na trhu a výrobce zařízení v rámci svého produktového portfolia taková zařízení nabízí (tzn. dodavatel je povinen vždy dodat takové zařízení, ve kterém výrobce zařízení používá k datu podání nabídky nejnovější verzi SW příslušenství). K dodanému SW příslušenství musí být dostupná bezplatná plnohodnotná technická podpora. Součástí technické podpory musí být průběžné provádění aktualizací SW (update, upgrade), včetně zajišťování aktualizace zabezpečení, opravy hotfix atd. Technická podpora musí být zajištěna bezplatně po dobu platnosti uzavřené servisní smlouvy. V případě, že v průběhu platnosti servisní smlouvy bude ze strany výrobce SW ukončena celosvětově technická podpora a dodavatel nebude schopen z technických důvodů zajistit u dodaného zařízení bezplatný upgrade na novější verzi systému s platnou technickou podporou, bude dodavatel povinen v rámci servisní činnosti povinen zajistit bezplatně kybernetickou bezpečnost na zadavatelem stanovenou minimální úroveň (např. prostřednictvím dodání a instalace dalších bezpečnostních prvků ve vztahu k možnosti setrvání připojení dodaného zařízení k síti zadavatele).

V případě, že dodavatel nemůže tyto standardy dodržet (z technologických důvodů), musí být realizována taková opatření, aby byly naplněny požadavky kybernetické bezpečnosti. Na odchylky proti standardu je třeba v nabídce zařízení zřetelně upozornit.

Zejména:

Pokud nelze počítač/zařízení spravovat centrálním desktop managementem, musí dodavatel zajistit minimálně 2x ročně aktualizaci dostupných aktualizací výrobce operačního systému a aplikace na vlastní náklady.

Pokud počítačový systém/dodaný SW vykazuje známé bezpečnostní chyby, které nelze opravit bezpečnostními záplatami nebo aktualizacemi, dodavatel doplní lokální firewall s logováním přístupu na vlastní náklady.

Pokud nelze na počítači/zařízení pracovat s doménovými účty s právy USERS bude ve spolupráci s OITPaR zakázán přístup počítače na internet. Pokud technologie potřebuje přístup na internet, dodavatel musí specifikovat cíl přístupu pomocí FQDN (např. www.domena.cz).

Lokální účet s právy USERS nutný pro běh systému musí odpovídat bezpečnostním standardům GA ČR, délka minimálně 12 míst, velká a malá písmena, čísla, speciální znaky, změna hesla minimálně 1x za 18 měsíců zajistí dodavatel ve spolupráci s OITPaR.

Pokud nelze na počítači/zařízení provozovat antivirový program GA ČR, dodavatel zajistí softwarové vypnutí volných USB portů.

Pokud výrobce nepovoluje ICMP PING, musí uchazeč akceptovat bezplatné výjezdy techniků při problémech na datové síti.