Dodatek č. 1

ke smlouvě o poskytování služeb servisu a údržby ekonomického, mzdového a personálního systému formou služby (SaaS)

(dále jen „**Dodatek**“)

Smluvní strany

1. Česká republika – Digitální a informační agentura
se sídlem: Na vápence 915/14, Praha 130 00
IČO: 17651921
Bankovní spojení:
Číslo účtu:
Zástupce: Ing. Martin Mesršmíd, ředitel

(dále označovaný jako „**Objednatel**“)

a

2. GORDIC spol. s r.o.
se sídlem: Erbenova 2108/4, Jihlava, PSČ: 586 01
IČO: 47903783
společnost zapsaná ve vložce č. 9313 oddílu C, obchodního rejstříku vedeného Krajským soudem v Brně
DIČ: CZ47903783
Bankovní spojení:
Číslo účtu:
Zástupce: Ing. Jaromír Řezáč, DBA, jednatel

(dále označovaný jako „**Poskytovatel**“)

(Objednatel a Poskytovatel označováni společně dále jako "**Smluvní strany**" nebo jednotlivě jako „**Smluvní strana**“)

Preambule

A. Smluvní strany mezi sebou dne 27. 12. 2023 uzavřely smlouvu o poskytování služeb servisu a údržby ekonomického, mzdového a personálního systému formou služby (SaaS), číslo smlouvy / č.j.: DIA-17255-2/OEZ-2023 („**Smlouva**“).

B. Smluvní strany se dohodly na níže ujednaných změnách Smlouvy a za tímto účelem se rozhodly uzavřít tento Dodatek.

Čl. 1 Úvodní ustanovení

1. Změny a ustanovení nově obsažená v tomto Dodatku se považují za vložená do Smlouvy a jako taková upravují příslušná ustanovení Smlouvy těmito změnami dotčená.

2. S výjimkou změn vyplývajících z tohoto Dodatku zůstává Smlouva v plném rozsahu platná a účinná.

Čl. 2 Změna Smlouvy

2. Smluvní strany se dohodly, že čl. 2 odst. 6 Smlouvy se nahrazuje následujícím zněním:

*„6. Poskytovatel poskytuje plnění ze Smlouvy sám, nikoliv prostřednictvím svých dodavatelů (dále jen „**poddodavatelé**“). Poskytovatel je oprávněn užít k plnění svých povinností poddodavatele pouze s předchozím písemným souhlasem Objednatele a pokud Poskytovatel zaváže poddodavatele mlčenlivostí a jinými vhodnými způsoby tak, aby nebyly ohroženy povinnosti Poskytovatele vyplývající z této Smlouvy a zaváže poddodavatele dodržovat v plném rozsahu ujednání mezi Objednatelem a Poskytovatelem.“*

3. Smluvní strany se dohodly, že čl. 2 odst. 8 l) Smlouvy se nahrazuje následujícím zněním:

„l) informovat Objednatele dopředu o i) významné změně kontroly nad Poskytovatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 74 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, či ekvivalentní postavení, ii) změně vlastnictví zásadních aktiv využívaných Poskytovatelem k plnění ze Smlouvy, a iii) změně oprávnění nakládat se zásadními aktivy využívanými Poskytovatelem k plnění ze Smlouvy.“

4. Smluvní strany se dohodly, že se do Smlouvy doplňuje nový čl. 4 odst. 8 v následujícím znění:

„8. V případě, že Poskytovatel poruší jakoukoliv svoji povinnost dle Kybernetických požadavků uvedených v Příloze č. 4 [Požadavky na zajištění kybernetické bezpečnosti] Smlouvy, má Objednatel nárok uplatnit smluvní pokutu ve výši 25 000 Kč, a to za každé jednotlivé porušení povinnosti Poskytovatele.“

5. Smluvní strany se dohodly, že čl. 9 odst. 4 Smlouvy se nahrazuje následujícím zněním:

„8. Objednatel je vlastníkem veškerých dat uložených v Systému včetně zákaznických dat a provozních údajů a Poskytovatel prohlašuje, že provedení exportu ze Systému je realizovatelné bez součinnosti Poskytovatele. Pro tyto účely má Systém definované široké spektrum možných výstupů, realizovatelných vlastními silami Objednatele. Poskytovatel je povinen veškerá data Objednatele nejpozději do třiceti (30) dnů po ukončení Smlouvy smazat způsobem, který je v souladu s použitelnými právními předpisy a regulatorními požadavky, a to ve všech systémech Poskytovatele. Poskytovatel o plánovaném smazání informuje Objednatele nejpozději do deseti (10) dnů po ukončení Smlouvy včetně informace o možnosti provedení exportu dat. Objednatel je oprávněn lhůtu pro smazání dat jednostranně prodloužit o dalších třicet (30) dní.“

6. Smluvní strany se dohodly, že se do Smlouvy za čl. 10 odst. 5 a) vii. doplňuje text v následujícím znění:

„viii. Poskytovatel poruší povinnost informovat Objednatele dopředu o i) významné změně kontroly nad Poskytovatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 74 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, či ekvivalentní postavení, ii) změně vlastnictví zásadních aktiv využívaných Poskytovatelem k plnění ze Smlouvy, a iii) změně oprávnění nakládat se zásadními aktivy využívanými Poskytovatelem k plnění ze Smlouvy;

ix. Objednatel vyjádří nesouhlas s i) významnou změnou kontroly nad Poskytovatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 74 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění

pozdějších předpisů, či ekvivalentní postavení, ii) změnou vlastnictví zásadních aktiv využívaných Poskytovatelem k plnění ze Smlouvy, a iii) změnou oprávnění nakládat se zásadními aktivy využívanými Poskytovatelem k plnění ze Smlouvy, a to třiceti (30) dnů ode dne, kdy se o dané okolnosti Objednatel dozvěděl."

7. Smluvní strany se dohodly, že se do Smlouvy doplňuje nový čl. 12 v následujícím znění:

„Čl. 12 Kybernetická bezpečnost

1. *Není-li v této Smlouvě nebo v souladu s touto Smlouvou stanoveno jinak, Poskytovatel tímto bere na vědomí, že:*
   a) *Objednatel je správcem informačních systémů kritické informační infrastruktury dle § 3 písm. c) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZKB**"), správcem komunikačního systému kritické informační infrastruktury dle § 3 písm. d) ZKB a správcem významných informačních systémů dle § 3 písm. e) ZKB. Poskytovatel dále tímto bere na vědomí, že poskytování Plnění dle této Smlouvy může být prováděno na aktivech systémů kritické informační infrastruktury a aktivech významných informačních systémů.*
   b) *Objednatel chápe Poskytovatele jako významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**VKB**").*

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

3. *Poskytovatel je povinen v rozsahu plnění této Smlouvy naplnit všechny bezpečnostní požadavky uvedené v Příloze č. 4 [Požadavky na zajištění kybernetické bezpečnosti] Smlouvy (dále jen „**Kybernetické požadavky**"), a to do termínu uzavření této Smlouvy. Poskytoval je povinen tyto požadavky udržovat naplněné po celou dobu trvání této Smlouvy.*

4. *Poskytovatel se zavazuje nad rámec auditu dle čl. 2 odst. 8 d) Smlouvy umožnit Objednateli alespoň jednou (1) ročně po dobu účinnosti této Smlouvy a jeden (1) kalendářní rok po ukončení Smlouvy provedení zákaznického auditu (kontroly):*
   a) *jehož rozsah bude ohraničen využíváním ICT prostředků Poskytovatele pro potřeby plnění této Smlouvy a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Poskytovatele; a*
   b) *jehož předmětem bude naplnění Kybernetických požadavků a vyhodnocení rizik dle bodu 3 Přílohy č. 4 [Požadavky na zajištění kybernetické bezpečnosti] Smlouvy.*

5. *Objednatel je oprávněn při kontrole Kybernetických požadavků využít třetí stranu. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám, včetně odpovědnosti za způsobenou škodu.*

6. *Poskytovatel se zavazuje umožnit Objednateli kontrolu Kybernetických požadavků provedenou prostředky Objednatele nebo třetí strany, a to v lokalitě Poskytovatele i vzdáleně, pokud to technické prostředky Poskytovatele umožňují.*

7. *Poskytovatel se nad rámec poskytování Plnění zavazuje poskytnout Objednateli součinnost minimálně v rozsahu deseti (10) člověkodnů při provádění každého zákaznického auditu ze strany Objednatele a pro tuto činnost zabezpečit účast kvalifikovaných pracovníků.*

8. *Dále se Poskytovatel zavazuje nedostatky zjištěné:*

   a) *na základě provedení hodnocení rizik dle bodu 3 v Příloze č. 4 [Požadavky na zajištění kybernetické bezpečnosti] Smlouvy a interních předpisů Objednatele nebo*

   b) *v rámci zákaznického auditu dle čl. 12 odst. 4 této Smlouvy*

   odstranit ve lhůtě určené v písemném oznámení Objednatele. Nestanoví-li Objednatel lhůtu v písemném oznámení, zavazují se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší devadesát (90) kalendářních dnů.

9. *Neodstranění nedostatků ve stanovené lhůtě je považováno za nenaplnění Kybernetických požadavků a tím porušení čl. 12 odst. 3.*

10. *Články 12 odst. 4 až odst. 7 této Smlouvy se nepoužijí, pokud je Poskytovatel pro poskytování Plnění dle této Smlouvy orgánem nebo osobou uvedenou v § 3 písm. a) až g) ZKB.*

11. *Poskytovatel se dále zavazuje:*

    a) *poskytnout na vyžádání a bez zbytečného odkladu Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků;*

    b) *na požádání s Objednatelem konzultovat kdykoli v průběhu poskytování Plnění dle této Smlouvy detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků;*

    c) *neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků, které nastanou kdykoli v průběhu trvání této Smlouvy;*

    d) *bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní;*

    e) *bezodkladně informovat Kontaktní osobu Objednatele o bezpečnostních incidentech, které mohou ovlivnit realizaci plnění dle této Smlouvy. Kontaktní osoby Smluvních stran vzájemně komunikují v průběhu poskytování Plnění dle Smlouvy za účelem dosažení standardů pro bezpečnost informací dle tohoto čl. 12. V případě ohrožení anebo porušení bezpečnosti informací, zejména v případě výskytu kybernetické bezpečnostní události anebo incidentu, jsou Kontaktní osoby povinny vzájemně komunikovat, ihned po zjištění takových skutečností hlásit jejich výskyt druhé Smluvní straně a společně podnikat kroky k zajištění obnovení bezpečnosti informací; a*

    f) *při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům, jejichž následkem bude či může být vznik škody anebo rozporu s obecně závaznými právními předpisy. Jestliže Poskytovatel při plnění Smlouvy zjistí či jako odborník mohl a měl zjistit rozpor ustanovení interních předpisů Objednatele se ZKB, VKB anebo rozhodnutím či jiným pokynem NÚKIB, je povinen takový rozpor Objednateli neprodleně ohlásit a poskytnout Objednateli součinnost k jeho odstranění.*

12. *Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu předmětu plnění a v souladu s interními předpisy Objednatele, se kterými byl Poskytovatel seznámen.*

13. *Povinnosti Poskytovatele vyplývající z tohoto čl. 12 platí adekvátně k podílu na poskytování Plnění i pro poddodavatele.“*

Čl. 3 Všeobecná a závěrečná ustanovení

1. Dodatek je podepsán a vyhotoven v elektronické podobě a podepsán platnými zaručenými elektronickými podpisy v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, s tím, že každá Smluvní strana obdrží Dodatek v elektronické podobě s uznávanými elektronickými podpisy.
2. Smluvní strany shodně prohlašují, že si tento Dodatek před jeho podpisem přečetly a že byl uzavřen po vzájemném projednání podle jejich pravé a svobodné vůle určitě, vážně a srozumitelně, nikoliv v tísni nebo za nápadně nevýhodných podmínek, a že se dohodly o celém jeho obsahu, což stvrzují svými podpisy.
3. Vztahy vznikající z Dodatku a v něm výslovně neupravené se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.
4. Tento Dodatek je nedílnou součástí Smlouvy.
5. Nedílnou součástí Dodatku jsou následující přílohy:
    - Příloha č. 1 Požadavky na zajištění kybernetické bezpečnosti.

   Příloha č. 1 Dodatku se stane přílohou č. 4 Smlouvy.

Objednatel	**Poskytovatel**
V Praze dne „dle elektronického podpisu“	V Praze dne „dle elektronického podpisu“
.....	.....
Česká republika – Digitální a informační agentura	**GORDIC spol. s r.o.**
Ing. Martin Mesršmíd	Ing. Jaromír Řezáč, DBA
Ředitel	Jednatel

Příloha č. 1

Příloha č. 4 Smlouvy Požadavky na zajištění kybernetické bezpečnosti

Za účelem plnění povinností stanovených Objednateli, jakožto povinné osobě dle VKB, je Poskytovatel povinen, nad rámec povinností stanovených v těle Smlouvy, plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této Přílohy.

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, avšak vždy pouze za účelem zajištění plnění povinnosti Poskytovatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

KYBERNETICKÉ POŽADAVKY

Bod 1 Systém řízení bezpečnosti informací

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění povinností uvedených v § 3 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel 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 této Smlouvy.
    b. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění této Smlouvy, monitorovat je, vyhodnocovat jejich účinnost.
    c. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění této Smlouvy, 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 této Smlouvy. 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.

Bod 2 Řízení aktiv

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy 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 této smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle této Smlouvy, 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 platnosti této Smlouvy a následně na vyžádání, a to po celou dobu trvání Smlouvy a po dobu dvou (2) let po jejím ukončení.

Bod 3 Řízení rizik

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy 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 této Smlouvy.
   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.

Bod 4 Organizační bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění povinností uvedených v § 6 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. 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 této Smlouvy pouze oprávněných osob, které byly řádně seznámeny s příslušnými interními předpisy Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.

Bod 5 Řízení poddodavatelů

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy aktivně podílet na splnění povinností uvedených v § 8 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. Využívá-li při poskytování předmětu plnění této Smlouvy Poddodavatele, zabezpečit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Poskytovatel zavazuje doložit Objednateli do deseti (10) dnů ode dne jejich zapojení do poskytování Plnění, písemným prohlášením Poskytovatele o dodržování Kybernetických požadavků u svých poddodavatelů.
   b. Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zabezpečit nad rámec čl. 8 Smlouvy uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění) ve smyslu příslušných ustanovení GDPR.

Bod 6 Bezpečnost lidských zdrojů

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy 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 platnosti Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění této Smlouvy za Poskytovatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních předpisů Objednatele.
   b. Dodržovat příslušná ustanovení interních předpisů Objednatele v rozsahu, v jakém byl s těmito interními 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 této Smlouvy.

d. Zabezpečit, aby osoby podílející se na poskytování plnění této Smlouvy 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;

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 této Smlouvy. Pokud nebude Objednateli umožněno osobní údaje dotčených pověřených osob Poskytovatele zpracovat, nebude těmto pověřeným osobám umožněn žádný přístup ke zdrojům Objednatele.

Bod 7 Řízení provozu a komunikací

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy 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 této Smlouvy.

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 této Smlouvy 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.

Bod 8 Řízení změn

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy 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.

Bod 9 Řízení přístupu

1. Poskytovatel se bude v rozsahu předmětu plnění Smlouvy aktivně podílet na splnění povinností uvedených v § 12 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje:
   a. Zavést pravidla řízení přístupů k Systému.
   b. Přidělovat oprávnění svým jednotlivým pověřeným osobám ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele a podle principu need-to-know.
   c. 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 této Smlouvy a dva (2) roky po jejím ukončení.
   d. 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).
   e. 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.
   f. 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 přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.
3. 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).

Bod 10 Akvizice, vývoj a údržba

1. Poskytovatel se bude v rozsahu předmětu plnění této Smlouvy 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, které jsou předmětem plnění Smlouvy, ledaže tyto činnosti provádí Objednatel.
   b. Předat Objednateli v přiměřené lhůtě stanovené Objednatelem dokumentaci předmětu plnění Smlouvy 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 této Smlouvy 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 v této Smlouvě stanoveno jinak, a to zejména za

účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu se smlouvou 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 plnění této Smlouvy bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru anebo které jsou specifikovány výslovně ve Smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

e. Pokud je součástí plnění této Smlouvy i instalace operačního systému případně softwaru třetích stran, zabezpečit 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 testovacích dat poskytnutých Objednatelem.

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

h. Zabezpečit, že v rámci poskytovaného plnění Smlouvy 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.

Bod 11 Zvládání kybernetických bezpečnostních událostí a incidentů

1. Poskytovatel se bude v rozsahu předmětu plnění Smlouvy 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. Zavést a využívat nástroje pro detekci, sběr a vyhodnocování kybernetických bezpečnostních událostí a incidentů.

   c. Bez zbytečného odkladu, nejpozději ale do 72 hodin od okamžiku, kdy se o narušení bezpečnosti Poskytovatel dozvěděl 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.

   d. Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

e. V případě vzniku bezpečnostní události 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.

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

g. 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.

2. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako vyšší moc vylučující povinnost k náhradě újmy Poskytovatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Poskytovatele za prodlení obsažená v Smlouvě nejsou tímto ustanovením dotčena.

Bod 12 Řízení kontinuity činností

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

   a. Zabezpečit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění Smlouvy.

   b. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané úrovně Plnění.

Bod 13 Kontrola a audit

1. Poskytovatel se bude v rozsahu předmětu plnění Smlouvy 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.

Bod 14 Fyzická bezpečnost

1. Poskytovatel se bude v rozsahu předmětu plnění Smlouvy 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 Smlouvy zabezpečit 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.

Bod 15 Bezpečnostní nástroje

1. Poskytovatel se bude v rozsahu předmětu plnění Smlouvy 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 a bezpečnosti komunikační sítě.

b. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.

c. Připojovat do IT prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobu ve věcech technických na straně Objednatele.

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 Smlouvy:

   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 Smlouvy, a to po celou dobu trvání Smlouvy a po dobu dvou (2) let po jejím ukončení.

i. Zabezpečit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění Smlouvy 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, pokud tato Smlouva nestanoví jinak.