PŘÍLOHA Č. 7 – KYBERNETICKÁ BEZPEČNOST

Článek I.

Úvodní ustanovení

1. Objednatel informuje Zhotovitele, že je osobou, která je povinna podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a v souladu s vyhláškou 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), zavést a provádět příslušná bezpečnostní opatření jako správce významného informačního systému, a to v rozsahu nezbytném pro zajištění kybernetické bezpečnosti.
2. Vyhláška o kybernetické bezpečnosti uvádí, že každý, kdo s povinnou osobou vstupuje do právního vztahu, jenž je významný z hlediska bezpečnosti informačního systému, je „významným dodavatelem“.
3. Objednatel jako „povinná osoba“ ve smyslu vyhlášky o kybernetické bezpečnosti též v rámci zavedení a provádění bezpečnostních opatření řídí Zhotovitele v souladu s ustanovením § 8 vyhlášky a odpovídá za stanovení pravidel pro Zhotovitele, která zohledňují požadavky systému řízení bezpečnosti informací.
4. Objednatel tímto dle § 8 vyhlášky o kybernetické bezpečnosti prokazatelně písemně informuje Zhotovitel o tom, že je pro Objednatele, jako správce významného informačního systému určeného dle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů, významným dodavatelem ve smyslu zákona o kybernetické bezpečnosti a že Objednatel vede Zhotovitele v evidenci svých významných dodavatelů s těmito náležitostmi:

Identifikace správce:	IČO 41197518
Identifikace významného informačního systému správce:	CRP, CVON, RSZP, RPP
Identifikace významného dodavatele:	IČO 05211131

a tímto ho dále v této Příloze č. 7 seznamuje s obsahem pravidel pro významné dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací, a vyžaduje zajištění plnění těchto pravidel Zhotovitelem.

5. Účelem této Přílohy č. 7 smlouvy je dodržet povinnost Objednatele dle § 8 vyhlášky o kybernetické bezpečnosti, zajistit, aby smlouva uzavíraná s významným dodavatelem obsahovala relevantní oblasti uvedené v příloze č. 7 vyhlášky o kybernetické bezpečnosti, a stanovit způsoby a úrovně realizace bezpečnostních opatření a určit vzájemnou smluvní odpovědnost za zavedení a kontrolu bezpečnostních opatření. Relevantní oblasti dle přílohy č. 7 vyhlášky o kybernetické bezpečnosti jsou obsaženy v této Příloze č. 7 smlouvy a dále přímo v textu smlouvy, resp. v jejích dalších přílohách.
6. Zhotovitel se zavazuje, že se bude při poskytování plnění na základě této smlouvy aktivně podílet na splnění povinností uvedených ve vyhlášce o kybernetické bezpečnosti, které musí splnit Objednatel, a to v rozsahu předmětu plnění dle této smlouvy pro danou oblast kybernetické

bezpečnosti a dále se bude podílet na dodržování, provozu a rozvoji bezpečnostních opatření Objednatele.

Článek II.

Ustanovení o souladu s obecně závaznými právními předpisy

1. Objednatel a Zhotovitel konstatují, že tato Příloha č. 7 je v souladu s aktuálními právními předpisy v oblasti kybernetické bezpečnosti a směřuje k tomu, že dokument musí plnit aktuální legislativní požadavky v oblasti kybernetické bezpečnosti a v případě významných legislativních změn v této oblasti bude smluvními stranami dokument upraven, tj. bude novým požadavkům přizpůsoben.
2. Aktuálními právními předpisy v oblasti kybernetické bezpečnosti, s nimiž má být plnění Zhotovitele v souladu, jsou především tyto normativní právní akty:
   2.1. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů.
   2.2. Vyhláška 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).
3. Zhotovitel se k naplnění účelu právní úpravy v oblasti kybernetické bezpečnosti, reaktivních a bezpečnostních opatření, kybernetických bezpečnostních incidentů, jakož i likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli, zavazuje k dodržování relevantních povinností v rozsahu a způsobem takovým, aby byl naplněn účel právní úpravy, které tato stanovuje Objednateli jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě její změny. V případě takových změn právní úpravy je Objednatel oprávněn požadovat od Zhotovitele přiměřenou součinnost i nad rámec povinností stanovených v této Příloze č. 7 smlouvy, avšak vždy pouze ve smyslu shora uvedeném, a to za účelem zajištění plnění povinností Zhotovitele z oblasti kybernetické bezpečnosti.

Článek III.

Systém řízení bezpečnosti informací

1. Zhotovitel bere na vědomí, že Objednatel má zaveden systém řízení bezpečnosti informací dle zákona o kybernetické bezpečnosti.
2. Zhotovitel se v rámci oblasti zajištění systému řízení bezpečnosti informací zavazuje:
   2.1. Prosadit bezpečnostní zásady a procesy, které budou pokrývat bezpečnost dat a informací, jež mohou být vytvářeny a zpracovávány na straně Zhotovitele při poskytování předmětu plnění.
   2.2. Řídit vlastní rizika Zhotovitele, která mohou ovlivnit poskytování předmětu plnění.
   2.3. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je, vyhodnocovat jejich účinnost.
   2.4. Vytvořit bezpečnostní politiku Zhotovitele v českém nebo slovenském jazyce, která bude pokrývat relevantní bezpečnostní opatření zajišťující bezpečnost dat a informací, jež mohou být vytvářeny a zpracovávány na straně Zhotovitele při poskytování předmětu plnění podle smlouvy a v souvislosti s ním. Bezpečnostní politika Zhotovitele musí obsahovat hlavní zásady,

cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací (k tomu viz čl. IV., odst. 6. této Přílohy č. 7).

2.5. Výše uvedenou bezpečnostní politiku Zhotovitel uloží na určené úložiště Objednatele k odsouhlasení Objednateli. V případě odsouhlasení vytvořené politiky Zhotovitele Objednatelem je Zhotovitel při poskytovaném plnění povinen se odsouhlasenou politikou řídit.

2.6. Stanovit a udržovat aktuální opatření bezpečnosti ve formě organizačních a technických opatření, které zajišťují naplnění bezpečnostní politiky.

2.7. 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.

2.8. Nejpozději do jednoho roku od podpisu smlouvy vyhodnotit dodržování bezpečnostní politiky Zhotovitele a zprávu poskytnout Pověřené osobě Objednatele uvedené ve smlouvě čl. XIV., odst. 6., písm. a) (vedoucí projektu).

Článek IV.

Ustanovení o povinnosti dodržování bezpečnostní politiky

1. Zhotovitel je rovněž povinen dodržovat bezpečnostní politiky Objednatele, se kterými byl seznámen v rámci jednacího řízení (dále jen „relevantní bezpečnostní politiky“).
2. Relevantní bezpečnostní politiky zveřejní Objednatel Zhotoviteli na určeném interním úložišti Objednatele, k němuž umožní Zhotoviteli vzdálený přístup.
3. Aktualizace bezpečnostních politik příp. nové bezpečnostní politiky umisťuje Objednatel na určené interní úložiště Objednatele a o těchto změnách prokazatelně informuje Pověřenou osobu Zhotovitele uvedenou ve smlouvě čl. XIV., odst. 6., písm. b).
4. Zhotovitel je povinen se s novým zněním bezpečnostních politik prokazatelně seznámit a následně písemně informovat Objednatele, že toto prokazatelné seznámení učinil.
5. Zhotovitel se zavazuje využívat pro poskytování předmětu plnění pouze osob, které byly řádně seznámeny s relevantními ustanoveními bezpečnostní politiky Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění dle smlouvy.
6. Zhotovitel se zavazuje dodržovat tato bezpečnostní opatření:

   6.1. Zajistit, aby všechny osoby, které se budou podílet na poskytování předmětu plnění, byly nejpozději před zahájením plnění prokazatelně poučeny o jejich povinnostech, bezpečnostní politice a ustanoveních této Přílohy č. 7.

   6.2. Zajistit, aby se všechny osoby, které se podílejí na poskytování předmětu plnění, byly nejpozději do 10 pracovních dnů od oznámení Zhotoviteli o změně v dokumentech bezpečnostních politik Objednatele prokazatelně seznámeny s aktuálním zněním bezpečnostní politiky Objednatele.

   6.3. Dodržovat příslušná ustanovení bezpečnostních politik Objednatele a nejpozději do jednoho roku od uzavření smlouvy provést kontrolu dodržování bezpečnostních politik ze strany osob Zhotovitele, které se podílejí na poskytování předmětu plnění. O kontrole pořídit písemnou zprávu a tuto zaslat neprodleně Pověřené osobě Objednatele uvedené ve smlouvě čl. XIV., odst. 6., písm. a) (vedoucí projektu).

Článek V.

Řízení aktiv

Zhotovitel se v rámci oblasti řízení aktiv zavazuje identifikovat, hodnotit a evidovat relevantní aktiva Zhotovitele využívaná pro zajištění plnění smlouvy (aktivy se rozumí primární aktiva a podpůrná aktiva dle vyhlášky o kybernetické bezpečnosti) a jejich vazby, a tato aktiva předložit (viz § 4 vyhlášky o kybernetické bezpečnosti) na vyžádání Objednatele, a to po celou dobu trvání smlouvy a do tří měsíců po jejím ukončení.

Článek VI.

Ustanovení o bezpečnosti informací

Zhotovitel se může při plnění smlouvy setkat se všemi úrovněmi informací, kterých je Objednatel správce a která jsou předmětem smlouvy, resp. předmětem ochrany z hlediska bezpečnosti informací. Zhotovitel hodnotí tato aktiva v souladu se stupnicemi uvedenými v příloze č. 1 vyhlášky o kybernetické bezpečnosti a pro danou úroveň takového aktiva je povinen zajistit v prostředí Zhotovitele ochranu důvěrnosti, dostupnosti a integrity minimálně dle požadavků uvedených ve výše uvedené příloze, není-li ve smlouvě stanoven jiný vyšší požadavek na zajištění ochrany takového aktiva.

Článek VII.

Ustanovení o nakládání s daty

1. Ustanovení o tom, komu v rámci plnění data náleží, kdo k nim má primárně užívací právo, jakým způsobem má Zhotovitel s daty nakládat, jak k nim řídit přístup, jak bude s daty a provozními údaji naloženo po ukončení spolupráce, zejména zda, a v jaké podobě dojde k předání dat, a jakých, Objednateli nebo jaká data budou zlikvidována, upravuje zejména čl. XVIII. této Přílohy č. 7, dále Příloha č. 3 smlouvy - Standardy IS VZP – NIS a Smlouva o zpracování osobních údajů („ZOU“).
2. Zhotovitel je oprávněn předat provozní nebo jakékoli jiné údaje do třetí země nebo mezinárodní organizaci pouze na základě písemného pokynu Pověřené osoby Objednatele, popř. s jejím písemným souhlasem.

Článek VIII.

Ustanovení o ochraně práv duševního vlastnictví

1. Ustanovení upravující práva duševního vlastnictví vztahující se k plnění podle této smlouvy, resp. spojená s tímto plněním jsou obsažena zejména v čl. XII. smlouvy „Licenční ujednání“.

Článek IX.

Ustanovení o povinnosti informovat Objednatele

1. Zhotovitel je dle výkladu požadavků přílohy č. 7 vyhlášky o kybernetické bezpečnosti týkajících se obsahu smluv uzavíraných s významným dodavatelem povinen informovat písemně Objednatele o tom, jakým způsobem řídí Zhotovitel rizika v rozsahu, který se dotýká plnění smlouvy. K zajištění výše uvedeného požadavku Zhotovitel povinen předložit Objednateli tento dokument, tj. dokument uvádějící splnění této povinnosti, a to do 3 měsíců od nabytí účinnosti smlouvy.

2. Zhotovitel je povinen neprodleně informovat Objednatele o tom, jaká identifikoval rizika, jaká přijal opatření k jejich eliminaci a o tom, jaká jsou zbytková rizika související s plněním smlouvy. Tuto informaci předkládá minimálně 1x za půl roku Pověřené osobě Objednatele uvedené ve smlouvě čl. XIV., odst. 6., písm. a) (vedoucí projektu), případně na vyžádání Objednatele.
3. Zhotovitel je povinen neprodleně informovat Objednatele o významné změně ovládání Zhotovitele. Přičemž ovládáním se rozumí zejména ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení.
4. Zhotovitel je povinen neprodleně informovat Objednatele o změně skutečného majitele v evidenci skutečných majitelů (§ 118b a násl. zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřeneckých fondů).
5. Zhotovitel do tří měsíců od nabytí účinnosti smlouvy navrhne Objednateli způsob určování a definice zásadních aktiv Zhotovitele a identifikuje svá zásadní aktiva. Přičemž zásadními aktivy je třeba rozumět taková aktiva (zejm. programové a technické prostředky či informace, které jsou poskytovány, a zaměstnanci, kteří realizují předmět smlouvy), která jsou určitým způsobem zásadní pro realizaci smluvního závazku, kterými proudí informace Objednatele nebo skrze která je možné proniknout do systémů Objednatele, a jejichž vlastník tak může přímo či nepřímo ovlivňovat bezpečnost dotčeného informačního systému, příp. dalších propojených systémů, a informací v něm/nich obsažených.
6. Zhotovitel je povinen neprodleně informovat Objednatele o změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, používaných Zhotovitelem k plnění podle smlouvy s Objednatelem.
7. Objednatel si vyhrazuje právo jednostranně odstoupit od smlouvy v případě významné změny kontroly nad Zhotovitelem nebo změny kontroly nad zásadními aktivy využívanými Zhotovitelem k plnění podle smlouvy.

Článek X.

Ustanovení upravující řetězení dodavatelů

1. Zhotovitel odpovídá za to, že poddodavatel (poddodavatelé) bude dodržovat v plném rozsahu ujednání, jaká má sjednána Objednatel se Zhotovitelem uvedená v této Příloze č. 7 a jednání poddodavatele nebude v rozporu s požadavky Objednatele na Zhotovitele. O splnění této povinnosti je Zhotovitel povinen prokazatelně seznámit poddodavatele a následně o skutečnosti písemně informovat Pověřenou osobu Objednatele uvedenou ve smlouvě čl. XIV., odst. 6., písm. a) (vedoucí projektu) nejpozději před zahájením plnění příslušným poddodavatelem.
2. Zhotovitel bere na vědomí, že za plnění povinností uvedených v této Příloze č. 7 poddodavatelem odpovídá vůči Objednateli Zhotovitel.
3. V případě, že se vyskytne situace, kdy Zhotovitel není schopen zcela ovlivnit podmínky, za jakých jeho poddodavatel vykonává svou činnost (typicky v případech přeprodávání služeb nadnárodních korporací nebo v případech, kde je poddodavatel mateřská společnost či jiná společnost z koncernu, která poddodavateli jakožto své podřízené, obecně slabší entitě určuje, za jakých podmínek bude své služby poskytovat), může Zhotovitel přijmout stanovené obchodní podmínky poddodavatele za současného přijetí jiného způsobu řízení rizik ve vztahu k poddodavateli (tj. povinnost poddodavatele řídit se ujednáními Objednatele a Zhotovitele uvedenými v této Příloze č. 7). O této situaci je Zhotovitel povinen prokazatelně informovat Pověřenou osobu Objednatele uvedenou ve smlouvě čl. XIV., odst. 6., písm. a) (vedoucí projektu).

Článek XI.

Řízení provozu a komunikací

1. Zhotovitel se v oblasti řízení provozu a komunikací zavazuje dodržovat tato bezpečnostní opatření:

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

   1.2. Na vyžádání ve lhůtě, která nebude kratší než šest pracovních dnů, ledaže bude příslušným orgánem veřejné moci požadováno jinak, poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

   1.3. Zajistit, že pro poskytování předmětu plnění budou využívány pouze technické a programové prostředky, které neobsahují známé kritické zranitelnosti a jsou v souladu s platnou českou a evropskou legislativou.

2. Zhotovitel je dále povinen provést a zabezpečit dodržování následujících bezpečnostních opatření:

   2.1. Zavedení postupů pro ochranu zařízení používaných v rámci plnění Zhotovitele proti škodlivému kódu, řízení technických zranitelností v informačním systému, který je využíván k poskytování předmětu plnění dle smlouvy.

   2.2. Zavedení pravidel a postupů pro ochranu informací a dat.

   2.3. Stanovení pracovních postupů pro instalaci, spouštění, ukončování provozu technických aktiv Zhotovitele, řešení mimořádných stavů.

   2.4. Řízení přístupu k datům a systémům Zhotovitele, které spadají do rozsahu poskytování předmětu plnění.

Článek XII.

Ustanovení o řízení změn významného informačního systému

1. Zhotovitel je dále povinen v rámci svého plnění u všech změn významného informačního systému nebo v souvislosti s ním prováděných v rámci plnění přezkoumávat možné dopady změny na zajištění kybernetické bezpečnosti Objednatele. Přičemž ty změny, které mají nebo mohou mít vliv na kybernetickou bezpečnost a představují vysoké riziko, identifikuje jako významné změny a informuje, o potřebě jejich určení jako významné, prostřednictvím Pověřené osoby Objednatele uvedené ve smlouvě čl. XIV., odst. 6., písm. a) (vedoucí projektu).

2. U takto určených významných změn je Zhotovitel povinen dokumentovat řízení těchto významných změn a provádět u nich, za součinnosti Objednatele, analýzu rizik (přezkum možných dopadů změny) v souladu se zákonem o kybernetické bezpečnosti.

3. Dle výsledků analýzy rizik, které předkládá Zhotovitel Objednateli, navrhuje Zhotovitel opatření za účelem snížení všech nepříznivých dopadů spojených s takovou významnou změnou a předkládá návrh aktualizace bezpečnostní politiky a bezpečnostních dokumentů Objednatele dotčených změnou a přijatými opatřeními příp. aktualizuje bezpečnostní politiku Zhotovitele, aby odpovídala novému stavu po provedení významné změny.

4. Zhotovitel musí vždy před implementací významné změny do provozního prostředí Objednatele zajistit možnost navrácení do původního stavu, tj. stavu před implementací změny dle sjednané součinnosti.

Článek XIII.

Řízení přístupu

1. Zhotovitel se v oblasti řízení přístupu zavazuje dodržovat tato bezpečnostní opatření:

   1.1. Postupovat dle ustanovení Přílohy č. 2 smlouvy – „Podmínky pro přístup Zhotovitele do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR vč. jejich Přílohy č. 1“.

   1.2. Přidělovat přístupy a přístupová oprávnění osobám podílejícím se na plnění ve svém prostředí v minimálním nutném rozsahu potřebném pro jejich výkon práce, tj. tak aby byla minimalizována rizika narušení bezpečnosti aktiv Objednatele v prostředí Zhotovitele.

   1.3. Zajistit, aby takto přidělené přístupy nebyly sdíleny více osobami, tj. zajistit jednoznačnou identifikaci fyzické osoby.

   1.4. Pravidelně kontrolovat a vyhodnocovat oprávněnost přístupu a přístupových oprávnění osob podílejících se na plnění na straně Zhotovitele v prostředí Zhotovitele.

Článek XIV.

Akvizice, vývoj a údržba

1. Zhotovitel se v oblasti akvizice, vývoje a údržby zavazuje zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.
2. V případě, že předmět plnění zahrnuje vývoj informačního systému ve správě Objednatele, zavazuje se Zhotovitel:

   2.1. Pokud jsou softwarové auditní činnosti a předání zdrojového kódu k informačnímu systému součástí plnění dle smlouvy, umožní Zhotovitel Objednateli audit prováděného nebo provedeného plnění a na písemnou žádost Objednatele předloží Zhotovitel Objednateli vyvíjený zdrojový kód k informačnímu systému na provedení codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), a to zejména za účelem ověření skutečnosti, zda Zhotovitel postupuje či postupoval při poskytování plnění v souladu se smlouvou.

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

   2.3. Zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování informačního systému a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že informační systém nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

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

   2.5. Zajistit bezpečnost testovacího prostředí Zhotovitele a ochranu poskytnutých testovacích dat Objednatelem.

   2.6. Zajistit, že v rámci poskytovaného plnění bude vyvíjený informační systém v souladu s bezpečnostními politikami a standardy Objednatele.

2.7. Pokud je předmětem plnění instalace informačního systému, provede Zhotovitel instalaci pouze na základě Objednatelem předem schválených migračních postupů.

2.8. Zajistit správu zdrojových kódů bezpečnou formou zajišťující jeho integritu dle Přílohy č. 3 smlouvy - Standardy IS VZP – NIS.

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

Článek XV.

Ustanovení o povinnosti informovat o kybernetických bezpečnostních incidentech

1. Zhotovitel je povinen zavést proces zvládání kybernetických bezpečnostních událostí a incidentů v prostředí Zhotovitele a neprodleně hlásit Objednateli na e-mail bi@vzp.cz zjištěné kybernetické bezpečnostní události a incidenty související s plněním a které mohou nebo mají dopad na zajištění bezpečnosti dat a informací ve správě Objednatele a byly detekovány v prostředí Zhotovitele.
2. Zhotovitel se dále zavazuje dodržovat tato bezpečnostní opatření:
    - Podílet se na zvládání kybernetických bezpečnostních událostí a incidentů detekovaných v prostředí Objednatele.
    - Zajistit, že osoby Zhotovitele budou oznamovat neobvyklé chování informačního systému Objednatele zjištěného při plnění a podezření na jakékoliv zranitelnosti hlásit na e-mail bi@vzp.cz.
    - Bez zbytečného odkladu hlásit Objednateli všechny kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty s potenciálním negativním dopadem na Objednatele na e-mail bi@vzp.cz.
    - V případě vzniku kybernetické bezpečnostní události a následného zvládání a vyhodnocování kybernetického bezpečnostního incidentu a/nebo v případě podezření na kybernetický bezpečnostní incident poskytnout Objednateli aktivní součinnost a relevantní informace o podezřelém zařízení či osobě na straně Zhotovitele.
    - Bez zbytečného odkladu a po dohodě s Objednatelem realizovat opatření požadovaná Objednatelem v dohodnutých termínech ke snížení dopadu kybernetického bezpečnostního incidentu nebo zamezení pokračování kybernetického bezpečnostního incidentu.
    - Spolupracovat při prošetření a určení příčiny kybernetického bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Zhotovitel kybernetický bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
3. Zhotovitel bere na vědomí, že postup zvládání kybernetického bezpečnostního incidentu či jiný důsledek porušení bezpečnostních opatření, jehož příčina je na straně Zhotovitele, nebude posuzován jako okolnost vylučující odpovědnost Zhotovitele za prodlení s řádným a včasným plněním předmětu smlouvy a nebude důvodem k jakékoli náhradě případné újmy Zhotoviteli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Zhotovitele za prodlení obsažená ve smlouvě nejsou tímto ustanovením dotčena.
4. Zhotovitel je povinen informovat Objednatele v případě zjištění případů porušení stanovených bezpečnostních opatření a dodržování bezpečnostních politik Objednatele i Zhotovitele ze strany osob, které se podílejí na plnění.

Článek XVI.

Ustanovení o specifikaci podmínek pro řízení kontinuity činností

1. Zhotovitel bere na vědomí, že po dobu jeho fungování vůči Objednateli bude zahrnut do plánů kontinuity či do relevantních havarijních plánů Objednatele, které se vztahují k poskytování předmětu plnění smlouvy.
2. Zhotovitel je povinen se formou součinnosti zapojit do řízení kontinuity činností Objednatele.
3. Zhotovitel je povinen zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.

Článek XVII.

Ustanovení o specifikaci podmínek pro formát předávání dat, provozních údajů a informací

1. Pro období plnění smlouvy, a i v případě ukončení spolupráce Objednatele se Zhotovitelem musí být Zhotovitelem předávaná data a provozní údaje Objednateli tak, aby byly pro Objednatele použitelné, tj. v čitelném formátu dat (pokud Objednatel nestanoví jinak), kde bude zaručena použitelnost v případě migrace.
2. Specifikace podmínek pro předání dat, provozních údajů a informací upravují ustanovení čl. II. smlouvy a dále Příloha č. 3 - Standardy IS VZP – NIS.
3. Objednatel si vyhrazuje právo dodatečně zpřesnit / nově určit formát předávání dat, provozních údajů a informací a další podrobnosti jejich předávání (příp. mechanismy pro jejich dodatečné určení) mezi Objednatelem a Zhotovitelem v případě potřeby dalších alternativ předávání dat, provozních údajů a informací, které mohou nastat v průběhu plnění smlouvy.

Článek XVIII.

Ustanovení o pravidlech pro likvidaci dat

1. Zhotovitel je povinen minimálně čtyři měsíce před ukončením smlouvy s Objednatelem předložit Objednateli písemný návrh způsobu mazání nepotřebných dat a způsobu likvidace technických nosičů informace, provozních údajů, informací a jejich kopií, které vznikly po dobu trvání smlouvy s Objednatelem a jsou uloženy či zpracovávány u Zhotovitele, k souhlasu Objednatele se způsobem bezpečné likvidace/mazání dat. Přičemž návrh Zhotovitele musí být předložen v souladu s platnou vyhláškou o kybernetické bezpečnosti a způsob likvidace/mazání dat by měl být stanoven v návaznosti na jejich citlivost a důležitost.
2. Zhotovitel je poté povinen na své náklady do jednoho měsíce po ukončení spolupráce s Objednatelem zajistit za přítomnosti Objednatele bezpečné mazání/likvidaci těchto dat minimálně všech provozních údajů a jejich kopií, které vznikly po dobu trvání smlouvy a jsou uloženy u Zhotovitele, dle Objednatelem odsouhlaseného způsobu likvidace/mazání dat a doložit Objednateli protokol o zajištění bezpečné likvidaci/mazání dat.

Článek XIX.

Ustanovení o kontrole a auditu Zhotovitele

1. Zhotovitel tímto bere na vědomí povinnost Objednatele dle § 8 odst. 1. písm. g) vyhlášky o kybernetické bezpečnosti, pravidelně přezkoumávat plnění smluv s významnými dodavateli z hlediska systému řízení bezpečnosti informací a provádět dle § 8 odst. 2. písm. b) vyhlášky o kybernetické bezpečnosti kontrolu zavedení bezpečnostních opatření.
2. Zhotovitel tímto bere na vědomí, že si Objednatel vyhrazuje právo provádět zákaznické audity Zhotovitele, přičemž tento audit může být proveden pomocí vlastních zdrojů nebo pomocí třetí strany.
3. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by audit kybernetické bezpečnosti prováděl sám, včetně odpovědnosti za způsobenou újmu.
4. Předmětem auditu bude kontrola plnění všech relevantních povinností, ke kterým se Zhotovitel touto přílohou smluvně zavázal, především půjde o kontrolu způsobu plnění dohodnutých bezpečnostních opatření uvedených v této Příloze č. 7, způsobu řízení dodavatelů, způsobu nakládání s daty, způsobu identifikace a hlášení kybernetických bezpečnostních incidentů, kontrolu dodržování bezpečnostních politik Objednatele i Zhotovitele, kontrolu způsobu řízení rizik na straně Zhotovitele v rozsahu, který se dotýká plnění smlouvy apod.
5. Objednatel tímto níže stanovuje základní pravidla zákaznického auditu Zhotovitele.
6. Zhotovitel umožní Objednateli provedení auditu kybernetické bezpečnosti u Zhotovitele, pokud o to Objednatel požádá.
7. Zhotovitel umožní Objednateli provedení auditu vždy při významné změně ve smyslu § 2 vyhlášky o kybernetické bezpečnosti, pokud se bude týkat Zhotovitele, v rámci jejího rozsahu.
8. Audit kybernetické bezpečnosti bude proveden osobou vyhovující podmínkám stanoveným v § 7 odst. 4 vyhlášky o kybernetické bezpečnosti, která bude nezávisle hodnotit správnost a účinnost zavedených bezpečnostních opatření.
9. Zhotovitel je povinen umožnit Objednateli audit kybernetické bezpečnosti provedený prostředky Objednatele nebo třetí strany, a to v lokalitě Zhotovitele i vzdáleně, pokud to technické prostředky Zhotovitele umožňují.
10. Zhotovitel je povinen odstranit nedostatky zjištěné v rámci auditu kybernetické bezpečnosti ve lhůtě určené v písemném oznámení Objednatele, která nebude kratší než dvacet (20) pracovních dnů. Nestanoví-li Objednatel lhůtu v písemném oznámení, Smluvní strany se zavazují dohodnout na lhůtě pro odstranění nedostatku, která nebude delší než šedesát (60) pracovních dnů.
11. Zhotovitel je povinen poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění bezpečnostních opatření.
12. Zhotovitel je povinen neprodleně informovat Objednatele o všech významných změnách v naplnění kybernetických požadavků, které nastanou kdykoli v průběhu trvání této smlouvy.
13. Objednatel s dostatečným předstihem alespoň 5 pracovních dnů oznámí Zhotoviteli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že Objednatel se zavazuje postupovat tak, aby nenarušil provozní potřeby Zhotovitele.
14. Objednatel si v případě závažných důvodů (např. podezření na rizikové chování Zhotovitele) v souvislosti s plněním této smlouvy vyhrazuje právo provést neohlášený audit u Zhotovitele s přihlédnutím k provozní situaci Zhotovitele.

15. Dokumentace auditů prováděných Objednatelem je vedena auditorem kybernetické bezpečnosti Objednatele. Záznamy týkající se určitého auditu jsou vždy označovány stejným identifikátorem. Jednotlivé záznamy auditů tvoří:
    - plán auditu,
    - oznámení o auditu,
    - dotazník k auditu (seznam otázek auditora, pokud auditor uzná za vhodné),
    - zpráva z auditu,
    - písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem (pokud je nezbytné pro dokumentování nálezů),
    - záznam o zjištění (nápravných opatřeních a následné kontrole).
16. Zhotovitel, jako auditovaná strana obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění.
17. Zhotovitel navrhne na základě zjištění uvedených v závěrečné auditní zprávě návrh opatření a termíny řešení a předá jejich seznam Objednateli k odsouhlasení.
18. V případě, že Objednatel nebude souhlasit s návrhem opatření nebo s termíny řešení, je Zhotovitel povinen návrh opatření nebo s termíny řešení odpovídajícím způsobem upravit.
19. Souhlas s navrženými opatřeními a termíny řešení potvrdí Objednatel písemně.
20. Zhotovitel má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření.
21. Zprávu o realizovaných opatřeních Zhotovitel oznamuje a předává Objednateli.

Článek XX.

Fyzická bezpečnost

1. Zhotovitel se zavazuje v prostředí Objednatele dodržovat interní předpisy Objednatele se kterými byl seznámen, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, nebo datové nosiče.
2. V rozsahu poskytovaného předmětu plnění dle smlouvy se Zhotovitel zavazuje zajistit fyzické zabezpečení, zejména označení, uchování a likvidaci, instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv, které jsou v držení Zhotovitele.

Článek XXI.

Technická opatření

1. Zhotovitel se v oblasti technických opatření mj. zavazuje dodržovat bezpečnostní opatření dle příslušných Standardů IS VZP – NIS, a dále zejména:
    1.1. Realizovat opatření pro odstranění nebo blokování síťového/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity a bezpečnosti komunikační sítě.
    1.2. Připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem, a jejich připojení bylo schváleno Objednatelem.

1.3. Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění dle smlouvy a je ve správě Zhotovitele.

1.4. Na aktiva Objednatele bez jeho předchozího písemného souhlasu neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění:

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

b) Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

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

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

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

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

1.6. Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu poskytovaného předmětu plnění, a to po celou dobu trvání plnění a pak po dobu dvou let po ukončení plnění.

1.7. Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu poskytovaného předmětu plnění smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

1.8. Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu.

2. Zhotovitel bere na vědomí, že v případě, kdy technické spojení ze strany Zhotovitele narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění.

3. Zhotovitel bere na vědomí, že veškeré aktivity Zhotovitele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu poskytovaného předmětu plnění a v souladu s bezpečnostními politikami Objednatele, případně s dalšími dokumenty, které byly Zhotoviteli zpřístupněny k seznámení.

Článek XXII.

Ustanovení o sankcích

1. Zhotovitel je povinen zaplatit Objednateli smluvní pokutu ve výši 200.000 Kč (slovy: dvě stě tisíc korun českých) v každém jednotlivém případě porušení povinnosti v oblasti kybernetické bezpečnosti vymezené v této Příloze č. 7, a to i opakovaně. Ujednáním o smluvní pokutě ani zaplacením smluvní pokuty není dotčeno právo Objednatele na náhradu újmy vzniklé z porušení povinnosti, ke kterému se smluvní pokuta vztahuje.