Evidenční číslo přidělené z Centrální evidence smluv: 150100

DODATEK Č. 1
KE SMLOUVĚ O POSKYTOVÁNÍ SLUŽEB

Smluvní strany:

Česká republika – Ministerstvo životního prostředí

Se sídlem:	Vršovická 1442/65, 100 00 Praha 10 – Vršovice
Zastoupenou:	Ing. Radomilem Mazačem, ředitelem odboru informatiky
IČO:	00164801
Bankovní spojení:	ČNB Praha 1
Číslo účtu:	7628001/0710
Zástupce pro věcná jednání:	Mgr. Jaromír Adamuška
	(tel.: +420 269 122 277, e-mail: jaromir.adamuska@mzp.gov.cz)

DÁLE JEN „**Objednatel**“
NA STRANĚ JEDNÉ,

a

SYSNET s.r.o.

se sídlem:	5. května 157, 250 64 Měšice
zastoupená:	Ing. Radimem Jägerem, jednatelem
IČO:	48026468
DIČ:	CZ48026468 (je plátcem DPH)
bankovní spojení:	Komerční banka Praha 5
číslo účtu:	7451430247/0100

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze sp. zn. 14242

DÁLE JEN „**Poskytovatel**“
NA STRANĚ DRUHÉ,

POSKYTOVATEL A OBJEDNATEL SPOLEČNĚ JEN „**Smluvní strany**“
NEBO JEDNOTLIVĚ „**Smluvní strana**“.

dnešního dne uzavřely tento dodatek v souladu s ustanovením § 1901 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**OZ**“)

(dále jen „**Dodatek**“)

1. ÚVOD

1.1 Smluvní strany uzavřely dne 31.08.2015 smlouvu o poskytování služeb (dále jen „**Smlouva**“), jejímž předmětem je závazek Poskytovatele provést v prostředí Objednatele jednorázovou technickou revizi systému IPPC a zabezpečit jeho systémovou podporu, a to na základě veřejné zakázky s názvem „Jednorázová technická revize systému IPPC a zabezpečení jeho systémové podpory“ s ev. č. 150100, ID VZ na tržišti GEMIN: T002/15/V00026605.

1.2 Objednatel jakožto správce významného informačního systému ve smyslu § 3 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZKB**“), informoval Poskytovatele o skutečnosti, že se stal jedním z provozovatelů tohoto informačního systému (Poskytovatel zabezpečuje funkčnost programových prostředků), a to prostřednictvím oznámení č. j. MZP/2024/110/186 ze dne 20. 02. 2024.

1.3 S ohledem na výše uvedené skutečnosti se Smluvní strany rozhodly na změně některých svých práv a povinností vyplývajících ze Smlouvy, a to pro zajištění souladu smluvního vztahu s aplikovatelnými právními předpisy, zejména ZKB a doprovodných předpisů.

1.4 Okamžikem nabytí účinnosti tohoto Dodatku se Dodatek stává společně s Přílohou nedílnou součástí Smlouvy a Smluvní strany jsou ustanoveními tohoto Dodatku a Přílohy vázány v plném rozsahu. V rozsahu, ve kterém nestanoví tento Dodatek jinak, zůstávají ustanovení Smlouvy a jejích příloh beze změny a Smluvní strany jsou jimi i nadále vázány.

2. ZMĚNA TEXTU SMLOUVY

2.1 Smluvní strany se v souladu s § 1901 OZ a odst. 8.5 Smlouvy a dále v souladu s § 222 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, dohodly na změně svých práv a povinností vyplývajících ze Smlouvy v rozsahu a za podmínek uvedených v tomto Dodatku.

2.2 Do Smlouvy se za přílohu č. 3 vkládá nová příloha č. 4 „*Pravidla kybernetické bezpečnosti*“, jejíž znění je uvedeno v příloze č. 1 k tomuto Dodatku („**Příloha**“) “) a za přílohu č. 4 se vkládá nová příloha č. 5 „*Pravidla pro dodavatele a bezpečnostní politiky*“ jejíž znění je uvedeno v příloze č. 2 k tomuto Dodatku. Odst. 8.10 Smlouvy se mění tak, že se na konec odstavce doplňuje následující znění:

„*d) Příloha č. 4 – Pravidla kybernetické bezpečnosti*“;

„e) Příloha č. 5 – Pravidla pro dodavatele a bezpečnostní politiky“.

2.3 Ve Smlouvě se v článku 4.2 nahrazuje Tabulka č. 2: Maximální odměna za jeden rok kompletní podpory celého systému (SLA):, a to následující tabulkou:

	Služba	Rozsah (člověkodny)	Sazba za člověkoděn	Odměna celkem bez DPH	DPH 21 %	Odměna celkem vč. DPH
1	**Servis**	**Paušální**		120.000,- Kč	25.200,- Kč	145.200,- Kč
2	**Změnové řízení**	**24**	4.800,- Kč	115.200,- Kč	24.192,- Kč	139.392,- Kč
3	**Konzultace**	**3**	4.800,- Kč	14.400,- Kč	3.024,- Kč	17.424,- Kč
4	**Profylaxe**	**Paušální**		29.000,- Kč	6.090,- Kč	35.090,- Kč
	Celkem			**278.600,- Kč**	**58.506,- Kč**	**337.106,- Kč**

2.4 Do Smlouvy se za článek 6 vkládá nový článek 7, který zní:

„*VII. KYBERNETICKÁ BEZPEČNOST*

7.1 Není-li v této Smlouvě nebo v souladu s touto Smlouvou stanoveno jinak, Poskytovatel tímto bere na vědomí, že:

*7.1.1 Objednatel je během trvání této Smlouvy povinnou osobou ve smyslu § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZKB**“). Poskytovatel dále tímto bere na vědomí, že poskytování Služeb je prováděno na aktivech významného informačního systému.*

7.1.2 Objednatel seznámil Poskytovatele se skutečností, že jej vyhodnotil a eviduje jako provozovatele a významného dodavatele. V případě, že se Objednatel stane správcem dalších regulovaných aktiv ve smyslu ZKB během trvání Smlouvy, zavazuje se Poskytovatele o uvedeném bez zbytečného odkladu informovat, pokud je dané relevantní pro poskytování Služeb a plnění Smlouvy.

7.2 Smluvní strany potvrzují, že rozsah zapojení Poskytovatele na zajištění bezpečnosti aktiv systému/ů ve smyslu odst. 7.1.1. je omezen předmětem této Smlouvy, resp. povahou Služeb.

*7.3 Poskytovatel je povinen v rozsahu plnění této Smlouvy přijmout všechna kybernetická bezpečnostní opatření specifikovaná v Příloze č. 4 a Příloze č. 5, resp. Dodatku č. 1 (dále jen „**Bezpečnostní opatření**“). Poskytovatel se dále zavazuje:*

7.3.1 poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Bezpečnostních opatření;

7.3.2 na požádání s Objednatelem konzultovat kdykoli v průběhu poskytování Služeb detailní nastavení Bezpečnostních opatření a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků; a

7.3.3 neprodleně informovat Objednatele o všech významných změnách v plnění Bezpečnostních opatření a s vyvinutím nejlepšího úsilí zajistit po konzultaci

s Objednatelem náhradní způsob naplnění Bezpečnostních opatření, pokud stávající řešení přestalo být bezpečné, funkční a/nebo efektivní.“

3. VÝKLADOVÁ USTANOVENÍ

3.1 Stanoví-li Příloha Smluvní straně závazek splnit určitou povinnost před podpisem Smlouvy a/nebo uzavřením tohoto Dodatku, je dotčená Smluvní strana povinna tuto povinnost splnit před uzavřením tohoto Dodatku. Stanoví-li Příloha Poskytovateli závazek splnit povinnost ve stanovené lhůtě od zahájení poskytování plnění dle Smlouvy, je Poskytovatel povinen tuto povinnost splnit v dané lhůtě ode dne uzavření tohoto Dodatku. Ostatní povinnosti je Poskytovatel povinen splnit ke dni nabytí účinnosti Dodatku nebo v případech a lhůtách výslovně stanovených v Příloze.

3.2 Poskytovatel je povinen po ukončení Smlouvy a při migraci postupovat také v souladu s čl. 9 Přílohy, zejména pak vypracovat Migrační plán v souladu s ustanovením odst. 9.2 Přílohy a společně s Migračním plánem předat Objednateli dokumentaci a informace v souladu s odst. 9.3 Přílohy.

3.3 Objednatel je pro komunikaci s Poskytovatelem dle Přílohy oprávněn využívat Service Desk dle Smlouvy.

3.4 Poskytovatel je povinen v rámci relevantních reportů dle Smlouvy poskytovat Objednateli informace ohledně plnění svých povinností dle Přílohy tam, kde Příloha vyžaduje průběžné nebo opakované poskytování informací při zachování frekvence dle Přílohy.

3.5 Dokumentace zpracovaná Poskytovatelem dle odst. 2.4 Přílohy, jakož i veškeré její aktualizace dle odst. 2.5 Přílohy a další výstupy, které je Poskytovatel povinen zpracovat dle Přílohy, podléhají relevantnímu akceptačnímu řízení dle Smlouvy.

3.6 Veškerá činnost Poskytovatele dle Přílohy je součástí Paušálních služeb Poskytovatele dle Smlouvy a odměna Poskytovatele za plnění veškerých jeho povinností uvedených v Příloze (včetně odměny za poskytnutí, zprostředkování nebo postoupení licence dle odst. 3.2 Přílohy), jakož i veškeré náklady Poskytovatele spojené s jejich plněním, je zahrnuta v ceně Paušálních služeb.

3.7 Dojde-li určitým jednáním Poskytovatele k porušení povinností dle Smlouvy a vznikne-li Objednateli právo na zaplacení smluvní pokuty dle Smlouvy i Přílohy, je Poskytovatel povinen zaplatit smluvní pokutu za každé jednotlivé porušení pouze jedenkrát, a to tu vyšší.

3.8 Ustanovení § 2913 odst. 2 OZ se pro škodu způsobenou porušením povinností uvedených v Příloze neuplatní.

3.9 Poskytovatel je povinen při plnění povinností ochrany Důvěrných Informací dle Smlouvy postupovat v souladu s odst. 2.6 až 2.13 a 2.15 Přílohy.

3.10 Data Objednatele se považují za Důvěrné Informace chráněné ve Smlouvě.

3.11 Skončením účinnosti Smlouvy nejsou dotčena relevantní ustanovení obsažená v Příloze, která mají dle své povahy trvat i po skončení účinnosti Smlouvy.

3.12 Pro účely Přílohy je Poskytovatel označen jako Dodavatel.

4. ZÁVĚREČNÁ USTANOVENÍ

4.1 Poskytovatel výslovně prohlašuje, že se s ustanoveními obsaženými v Příloze a Pravidlech pro dodavatele a bezpečnostních politikách seznámil (příloha č. 2

k tomuto Dodatku), a zavazuje se je dodržovat. Poskytovatel dále prohlašuje, že ke dni účinnosti tohoto Dodatku splňuje veškeré relevantní požadavky uvedené v Příloze.

4.2 Smluvní strany se dohodly, že v souladu s odst. 5.1 Přílohy se na Smluvní vztah neuplatní následující části Pravidel pro dodavatele a bezpečnostních politik:

4.2.1 Poskytovatel (SYSNET) není oprávněn v případě IS IPPC řídit přístup k provozním aktivům Objednatele. poskytovatel není provozovatelem systému ověřování totožnosti uživatelů IPPC, ani správy uživatelů.

4.2.2 Poskytovatel (SYSNET) nemá ve své správě provozní data IS IPPC.

4.3 Pojmy použité v tomto Dodatku uvozené velkým písmenem, které nejsou definované v tomto Dodatku, mají význam zavedený ve Smlouvě a Příloze.

4.4 Tento Dodatek a veškerá práva a povinnosti vznikající na jeho základě a ve spojitosti s ním se řídí právem České republiky.

4.5 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů, vzniklých na základě tohoto Dodatku nebo v souvislosti s tímto Dodatkem, a k jejich vyřešení zejména prostřednictvím jednání odpovědných osob nebo jiných pověřených subjektů. Nebudou-li vyřešeny smírně, všechny spory vznikající z tohoto Dodatku a v souvislosti s ním včetně sporů o jeho výklad či platnost budou rozhodovány příslušným soudem v České republice.

4.6 Pokud jakákoliv ustanovení nebo jakékoliv části ustanovení Dodatku budou považovány za neplatné, zdánlivé nebo nevymahatelné, nebude mít taková neplatnost, zdánlivost nebo nevymahatelnost za následek neplatnost, zdánlivost nebo nevymahatelnost celého Dodatku, ale celý Dodatek se bude vykládat tak, jako kdyby neobsahoval příslušná neplatná, zdánlivá nebo nevymahatelná ustanovení nebo části ustanovení a práva a povinnosti Smluvních stran se budou vykládat přiměřeně. Smluvní strany se dále zavazují, že budou navzájem spolupracovat s cílem nahradit takové neplatné, zdánlivé nebo nevymahatelné ustanovení platným a vymahatelným ustanovením, jímž bude dosaženo stejného ekonomického výsledku (v maximálním možném rozsahu v souladu s právními předpisy), jako bylo zamýšleno ustanovením, jež bylo shledáno neplatným či nevymahatelným.

4.7 Tento Dodatek je vyhotoven ve dvou (2) vyhotoveních, z nichž každé má platnost originálu. Každá ze Smluvních stran obdrží jedno (1) vyhotovení.

4.8 Smluvní strany souhlasí a berou na vědomí, že k dodržení formy právního jednání postačí elektronický podpis.

4.9 Tento Dodatek obsahuje úplné ujednání o předmětu Dodatku a všech náležitostech, které Smluvní strany měly a chtěly v Dodatku ujednat a které považují za důležité pro závaznost tohoto Dodatku. Žádný projev Smluvních stran učiněný při jednání o tomto Dodatku ani projev učiněný po uzavření tohoto Dodatku nesmí být vykládán v rozporu s výslovnými ustanoveními tohoto Dodatku a nezakládá žádný závazek žádné ze Smluvních stran.

4.10 Nedílnou součástí tohoto Dodatku je následující příloha:

4.10.1 Příloha č. 1 – Pravidla kybernetické bezpečnosti

4.10.2 Příloha č. 2 – Pravidla pro dodavatele a bezpečnostní politiky

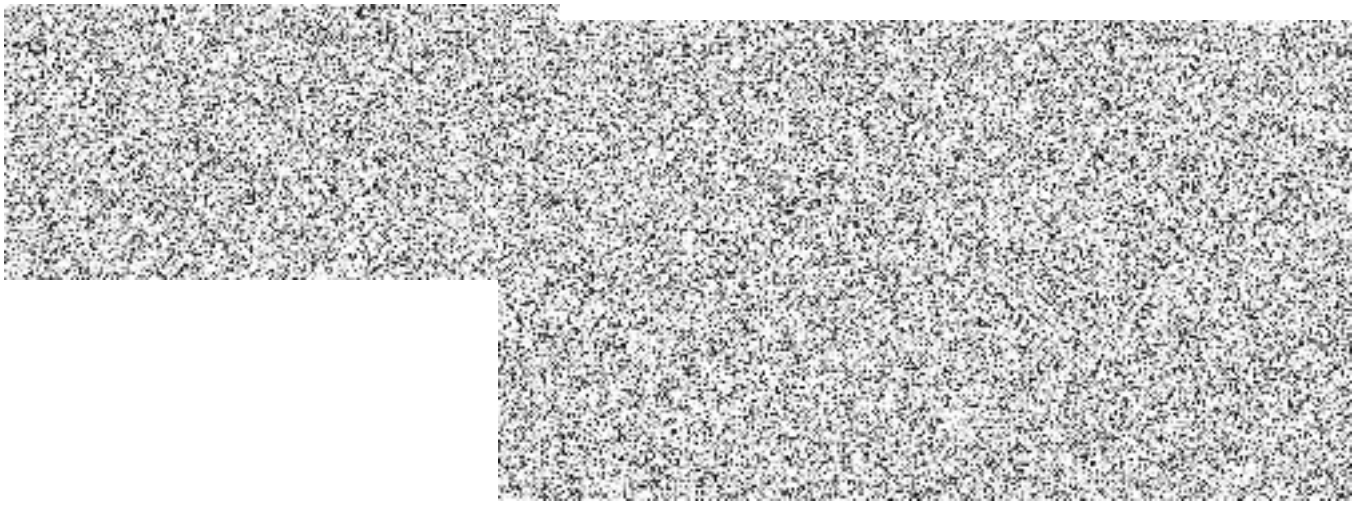
4.11 Smluvní strany bezvýhradně souhlasí s uveřejněním tohoto Dodatku v plném znění včetně veškerých metadat v souladu s příslušnými právními předpisy, které se na uveřejnění Smlouvy, resp. tohoto Dodatku vztahují, tj. zejména v souladu se

zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

4.12 Tento Dodatek nabývá platnosti dnem jeho podpisu oběma Smluvními stranami a účinnosti dnem jeho uveřejnění dle odst. 4.11 tohoto článku. Podle dohody Smluvních stran uveřejnění tohoto Dodatku provede Objednatel.

Smluvní strany prohlašují, že si tento Dodatek přečetly, že s jeho obsahem souhlasí a na důkaz toho k němu připojují svoje podpisy.

Za Objednatele:	Za Poskytovatele:
V _____ dne _____ 2025	V _____ dne _____ 2025
Ministerstvo životního prostředí	**SYSNET s.r.o.**
Jméno: Ing. Radomil Mazač	Jméno: Ing. Radim Jäger
Funkce: ředitel odboru informatiky	Funkce: jednatel



PŘÍLOHA Č. 1

PRAVIDLA KYBERNETICKÉ BEZPEČNOSTI

1. OBECNÁ USTANOVENÍ

1.1 Tato příloha (dále jen „**Příloha**“) tvoří nedílnou součást Smlouvy (dále jen „**Smlouva**“). Ustanovení těla Smlouvy mají přednost před ustanoveními této Přílohy.

1.2 Není-li dále stanoveno jinak nebo nevyplývá-li jinak z kontextu, mají pojmy počínající velkým písmenem v této Příloze shodný význam, jaký mají ve Smlouvě. Výjimkou je označení Zhotovitele/Poskytovatele, který je pro účely této Přílohy označován jako „**Dodavatel**“.

1.3 Smluvní strany nad rámec Smlouvy vymezují následující pojmy:

1.3.1 **Dodavatel** znamená Zhotovitel/Poskytovatel dle Smlouvy;

1.3.2 **ZKB** znamená zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů; a

1.3.3 **VKB** znamená vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

1.4 Dodavatel bere na vědomí, že jej Objednatel současně považuje za provozovatele dle § 2 písm. g) ZKB a eviduje jej v souladu s § 8 odst. 1 písm. b) VKB.

2. BEZPEČNOST INFORMACÍ

2.1 Rozsah zapojení Dodavatele na rozvoji a provozu primárních a podpůrných aktiv dle VKB je určen předmětem Smlouvy, jejími přílohami a touto Přílohou. Rozsah zapojení Dodavatele na zajištění bezpečnosti těchto aktiv je určen zejména touto Přílohou a Pravidly pro dodavatele a bezpečnostními politikami.

2.2 Dodavatel se zavazuje při nakládání s aktivy chránit jejich důvěrnost, dostupnost a integritu s ohledem na jejich povahu a klasifikaci. Dodavatel se zavazuje seznámit a pro klasifikaci aktiv užívat úrovně klasifikace Objednatele.

2.3 Dodavatel je povinen zavést vhodná opatření pro ochranu aktiv přiměřené úrovni jejich klasifikace. Konkrétně se Dodavatel zavazuje zavést alespoň následující opatření:

2.3.1 zajistit, aby k aktivům měli přístup pouze oprávněné osoby;

2.3.2 používat vhodné kryptografické metody pro ochranu dat při jejich přenosu a uložení;

2.3.3 pravidelně aktualizovat užívané software a systémy;

2.3.4 pravidelně školit své zaměstnance o bezpečnostních hrozbách a postupech.

2.4 Dodavatel je povinen zpracovat a do 20 pracovních dnů od zahájení poskytování plnění dle Smlouvy Objednateli předat dokumentaci zpracovanou v souladu s Pravidly pro dodavatele a bezpečnostními politikami Objednatele dle čl. 5, která bude ve vztahu k aktivům Objednatele ve smyslu přílohy č. 5 VKB zahrnovat alespoň:

2.4.1 postupy pro řízení provozu a komunikací;

2.4.2 postupy pro řízení přístupů (konkrétní postupy pro pracovníky Dodavatele podílející se na poskytování plnění dle Smlouvy);

2.4.3 postupy pro bezpečné chování uživatelů (konkrétní postupy pro pracovníky Dodavatele podílející se na poskytování plnění dle Smlouvy);

2.4.4 postupy pro zajištění bezpečnosti komunikační sítě;

2.4.5 postupy pro ochranu před škodlivým kódem;

2.4.6 postupy pro řízení změn alespoň v rozsahu stanoveném v čl. 6;

2.4.7 postupy pro zvládání incidentů;

2.4.8 pro řízení kontinuity činnosti;

2.4.9 další dokumentaci relevantní pro poskytování služby;

2.5 Dokumentaci podle odst. 2.4 této Přílohy je Dodavatel povinen revidovat a případně aktualizovat nejméně jednou ročně a dále kdykoli při změně skutečností zachycených v dokumentaci. Dodavatel je povinen výsledek provedené revize a případné aktualizace oznámit Objednateli bez zbytečného odkladu od jejich provedení.

2.6 Dodavatel nesmí používat nebo sdílet informace Objednatele a nesmí používat jiná aktiva Objednatele pro jiné účely a/nebo jiným způsobem, než jsou vymezeny ve Smlouvě a jejích přílohách.

2.7 Dodavatel je povinen omezit přístup k aktivům Objednatele pouze na ty zaměstnance a třetí strany, u kterých přístup vyžaduje plnění Smlouvy nebo plnění zákonných povinností. Dodavatel nesmí umožnit přístup k aktivům Objednatele jiným třetím stranám bez předcházejícího písemného souhlasu Objednatele.

2.8 Dodavatel souhlasí, že veškeré informace, dokumentace a databáze Objednatele, ke kterým bude mít Dodavatel přístup, případně informace a skutečnosti, které budou sděleny písemně, elektronicky či ústně Objednatelem nebo jeho zaměstnanci, členy statutárních orgánů, zmocněnci nebo poradci, Dodavateli nebo jeho zástupcům v souvislosti s plněním povinností ze Smlouvy, a to jak před podpisem tohoto Dodatku, tak i po jeho uzavření, jsou Objednatelem považovány za důvěrné (dále „**Důvěrné informace**“). Objednatel a Dodavatel také souhlasí, že za Důvěrné informace jsou považovány i veškeré informace a jakékoliv údaje obchodní, výrobní, technické či ekonomické povahy související s činností Objednatele, které nejsou veřejně dostupné. Zejména se jedná o informace týkající se autorských práv, počítačového softwaru, obsahu databází, veškeré údaje v softwarových aplikacích, účetních a daňových skutečností Objednatele. Důvěrnými informacemi se rovněž rozumí i takové informace, které Objednatel za důvěrné označí.

2.9 Dodavatel může použit Důvěrné informace pouze pro účely související s plněním povinností ze Smlouvy. Dodavatel se zavazuje zachovávat mlčenlivost o všech Důvěrných informacích Objednatele, o nichž se dozví v souvislosti s vykonáváním povinností pro Objednatele. Tento závazek trvá i po ukončení vykonávání povinností ze Smlouvy.

2.10 Dodavatel je oprávněn sdělit Důvěrné informace třetí osobě mimo své zaměstnance pouze s předchozím písemným souhlasem Objednatele, na základě písemné žádosti, ve které Dodavatel identifikuje třetí osobu a rozsah Důvěrných informací, které budou této třetí osobě sděleny. Dodavatel je však povinen zavázat tyto třetí osoby k mlčenlivosti minimálně ve stejném rozsahu, jako je sám zavázán v tomto

Dodatku. Dodavatel odpovídá Objednateli za porušení povinností těchto třetích osob ve stejném rozsahu, jako by je porušil sám.

2.11 Dodavatel se zavazuje postupovat při zacházení s Důvěrnými informacemi Objednatele nanejvýš obezřetně, aby nedošlo k jejich ztrátě, vyzrazení či zveřejnění třetím osobám, jejich znehodnocení, ani k jinému neoprávněnému zacházení s nimi, a to jak po dobu vykonávání povinností ze Smlouvy, tak i po jejich skončení.

2.12 Dodavatel se zavazuje, že poskytnuté Důvěrné informace nevyužije pro své účely či prospěch, ani pro účely a prospěch třetích osob, a ani tyto informace nepoužije žádným způsobem, kterým by mohl Objednatele poškodit, a to ani po ukončení Smlouvy.

2.13 V případě, že si Dodavatel bude vědom jakéhokoliv porušení závazku mlčenlivosti o Důvěrných informacích, neprodlené o tomto porušení písemně uvědomí Objednatele.

2.14 V případě, že Objednatel při hodnocení rizik spojených s touto Smlouvou identifikuje podstatná rizika, jejichž existence tvoří podstatnou kybernetickou hrozbu a riziko pro předmět této Smlouvy a dosahují kritické úrovně dle přílohy č. 2 VKB, může Objednatel Dodavateli uložit přijetí dalších bezpečnostních opatření ve smyslu § 5 ZKB bez nutnosti přijetí dodatku Smlouvy ve smyslu § 100 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Objednatel při naplnění podmínek výše předá Dodavateli seznam vybraných bezpečnostních opatření, která navrhuje ke snížení identifikovaného rizika zavést, a to včetně konkrétní specifikace formy bezpečnostního opatření. Dodavatel je povinen na své náklady bezodkladně zavést požadovaná bezpečnostní opatření a jejich zavedení oznámit Objednateli. Dodavatel je oprávněn do 3 pracovních dní podat připomínky k formě zvolených bezpečnostních opatření a navrhnout jinou formu zvolených bezpečnostních opatření, kterou je povinen zavést bezodkladně, po jejich schválení Objednatelem, a jejich zavedení Objednateli oznámit.

2.15 Učiní-li orgány činné v trestním řízení nebo jiné orgány státní správy jakoukoli právně závaznou žádost o poskytnutí informací Objednatele, je Dodavatel povinen tuto skutečnost oznámit Objednateli s předstihem před poskytnutím takových informací, pokud mu to právní předpisy nezakazují.

3. AUTORSTVÍ A LICENCE

3.1 Pokud bude výsledkem činnosti Dodavatele a součástí plnění Dodavatele dle Smlouvy dílo, které naplňuje znaky díla dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, a také v případě že bude jakékoli dílo naplňující tyto znaky autorského díla při plnění Smlouvy Dodavatelem použito, prohlašuje Dodavatel, že Dodavatel na základě Smlouvy a v souladu s ní získal veškerá potřebná oprávnění k takovému autorskému dílu, zejména je Dodavatel povinen zajistit, že Objednatel bude na základě Smlouvy a v souladu s ní oprávněn takové autorské dílo užít tak, aby byl splněn účel Smlouvy, včetně případného oprávnění k provádění změn a předání novému dodavateli v rámci převzetí činností při ukončení Smlouvy, a umožní převzetí činností Dodavatele při ukončení Smlouvy Objednatelem nebo jiným dodavatelem Objednatele.

3.2 Odměna za poskytnutí, zprostředkování nebo postoupení licence k autorskému dílu či za její zajištění je zahrnuta v ceně dle Smlouvy.

4. PODDODAVATELÉ A JEJICH ŘETĚZENÍ

4.1 Dodavatel se zavazuje, že plnění svých povinností vyplývajících ze Smlouvy, ve znění dodatků bude vykonávat výhradně sám a nebude užívat žádného poddodavatele nebo jinou třetí stranu.

5. PRAVIDLA PRO DODAVATELE A BEZPEČNOSTNÍ POLITIKY

5.1 Objednatel seznámil Dodavatele před podpisem Smlouvy se všeobecnými bezpečnostními požadavky na dodavatele z pohledu kybernetické bezpečnosti (dále jen „**Pravidla pro dodavatele a bezpečnostní politiky**“). Objednatel je oprávněn určit vybrané části Pravidel pro dodavatele a bezpečnostních politik, které se na Dodavatele nevztahují.

5.2 Dodavatel se Pravidla pro dodavatele a bezpečnostní politiky zavazuje dodržovat a seznámit s nimi pracovníky Dodavatele podílející se na poskytování plnění dle Smlouvy. Dodavatel odpovídá za zajištění dostatečné znalosti pravidel dle této Přílohy, jakož i Pravidel pro dodavatele a bezpečnostních politik ze strany svých pracovníků, a to včetně zajištění případných školení.

5.3 V případě změny Pravidel pro dodavatele a bezpečnostních politik se Objednatel zavazuje aktuální znění bez zbytečného odkladu od provedení změny předat Dodavateli. Objednatel zašle Dodavateli aktuální znění způsobem pro doručování dle Smlouvy nebo do datové schránky. Dodavatel se zavazuje v přiměřené lhůtě a ne později, než 10 pracovních dnů od předání Pravidel pro dodavatele a bezpečnostních politik protokolárně Objednateli potvrdit, že se s aktuálním zněním Pravidel pro dodavatele a bezpečnostních politik seznámil, že se je zavazuje dodržovat, včetně plnění povinností dle této Přílohy. Současně, pokud aktuální znění Pravidel pro dodavatele a bezpečnostních politik ukládá Dodavateli přijetí nových bezpečnostních opatření, stanoví Objednatel, po konzultaci s Dodavatelem, termín pro jejich zavedení a implementaci.

6. ŘÍZENÍ ZMĚN

6.1 Dodavatel je povinen poskytnout Objednateli veškeré potřebné informace a součinnost v procesu řízení a evidence změn v souladu s § 11 VKB. Informace musí být poskytnuty v rozsahu, který Objednateli umožní zejména:

6.1.1 posoudit, zda změna ve vztahu k plnění dle Smlouvy je významnou změnou ve smyslu § 2 písm. o) VKB;

6.1.2 posoudit rizika související s významnou změnou ve vztahu k plnění dle Smlouvy, testovat změnu před nasazením do provozu a posoudit možnost případného navrácení do původního stavu;

6.1.3 přijmout přiměřená opatření ke zvládání rizik souvisejících s touto změnou, nebo změnu vůbec neprovést, pokud nelze přijmout opatření snižující tato rizika na akceptovatelnou úroveň;

6.1.4 dokumentovat posouzení rizik souvisejících s významnou změnou ve vztahu k plnění dle Smlouvy a přijatá opatření; a

6.1.5 provést další činnosti u významných změn dle § 11 odst. 2 VKB.

7. SOULAD S PRÁVNÍMI PŘEDPISY

7.1 Smluvní strany se zavazují postupovat v souladu s relevantními obecně závaznými právními předpisy (dále jen „**Právní předpisy**“).

7.2 Právními předpisy se myslí zejména, nikoli však výlučně:

7.2.1 zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů;

7.2.2 zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů;

7.2.3 zákon č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů;

7.2.4 ZKB;

7.2.5 zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů;

7.2.6 zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů;

7.2.7 zákon č. 320/2001 Sb., o finanční kontrole, ve znění pozdějších předpisů;

7.2.8 zákon č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů;

7.2.9 zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů;

7.2.10 zákon č. 12/2020 Sb., o právu na digitální služby, ve znění pozdějších předpisů;

7.2.11 zákon č. 219/2000 Sb., o majetku České republiky, ve znění pozdějších předpisů;

7.2.12 zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů;

7.2.13 zákon č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů;

7.2.14 VKB;

7.2.15 vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích;

7.2.16 vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů;

7.2.17 vyhláška č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů;

7.2.18 vyhláška č. 168/2016 Sb., o uveřejňování formulářů pro účely zákona o zadávání veřejných zakázek a náležitostech profilu zadavatele, ve znění pozdějších předpisů;

7.2.19 nařízení Vlády č. 172/2016 Sb., o stanovení finančních limitů a částek pro účely zákona o zadávání veřejných zakázek, ve znění pozdějších předpisů;

7.2.20 nařízení Evropského parlamentu a Rady (EU) 2021/1060 ze dne 24. června 2021;

7.2.21 směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016;

7.2.22 směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022;

7.2.23 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016.

8. INFORMAČNÍ POVINNOST DODAVATELE

8.1 Dodavatel je povinen Objednatele bez zbytečného odkladu informovat o identifikovaných kybernetických bezpečnostních incidentech či jiných kybernetických hrozbách souvisejících s plněním Smlouvy, nejpozději však do 24 hodin od zjištění a identifikace jejich výskytu, a to prostřednictvím skupinového emailu masters@mzp.gov.cz nebo ServiceDesku.

8.2 Dodavatel je povinen Objednatele bez zbytečného odkladu informovat o způsobu řízení rizik na straně Dodavatele a o zbytkových rizicích souvisejících s plněním Smlouvy.

8.3 Dodavatel je povinen poskytnout Objednateli veškerou součinnost nutnou ke splnění povinností Objednatele v oblasti řízení rizik, zejména při:

8.3.1 identifikaci aktiv v rámci předmětu plnění Smlouvy a jejich kategorizaci, hodnocení a zařazení do bezpečnostních úrovní;

8.3.2 identifikaci, analýze a hodnocení rizik pro aktiva dle odst. 8.3.1;

8.3.3 ošetření rizik včetně zpracování prohlášení o aplikovatelnosti a plánu zvládání rizik pro aktiva dle odst. 8.3.1.

8.4 Při provádění úkonů podle odst. 8.3 této Přílohy je Dodavatel povinen postupovat podle metodik a postupů specifikovaných v Pravidlech pro dodavatele a bezpečnostních politikách, nebo pokud Pravidla pro dodavatele a bezpečnostní politiky tuto oblast neupracují, pak podle zavedených postupů v odvětví.

8.5 Zásadními aktivy dle odst. 13.2 této Přílohy jsou zejména aktiva, s pomocí nichž je možné přímo či nepřímo ovlivňovat bezpečnost systému a informací v něm obsažených, tedy aktiva, kterými proudí informace Objednatele či skrze která je možné proniknout do jeho systémů a která jsou zásadní pro realizaci Smlouvy.

9. UKONČENÍ SMLOUVY

9.1 Smluvní strany se dohodly, že při ukončení Smlouvy z jakéhokoli důvodu vyvinou veškeré úsilí k tomu, aby do převodu plnění dle Smlouvy k Objednateli nebo jinému provozovateli, nedošlo k narušení parametrů plnění ve Smlouvě do té doby definovaných, a aby případný nový provozovatel dostal veškeré informace o plnění Smlouvy potřebné pro pokračování nebo nahrazení takového plnění.

9.2 Součástí plnění dle odst. 9.1 je i povinnost Dodavatele provádět činnosti spočívajících v přípravě a předání předmětu plnění Smlouvy novému dodavateli Objednatele, poskytování součinnosti, dokumentace a informací novému dodavateli. Za účelem poskytování součinnosti při ukončení se Dodavatel zavazuje do 30 dnů od obdržení výzvy Objednatele vypracovat dle a na základě pokynů Objednatele plán vymezující veškeré podmínky pro převedení služeb či jejich příslušné části na nového dodavatele.

9.3 Dodavatel se zavazuje, bez ohledu na znění článku 10 Dodatku a pokud tak nebylo učiněno již dříve, do 30 dnů od obdržení výzvy Objednatele předat Objednateli:

9.3.1 aktualizovanou dokumentaci, kterou vytvořil nebo spravuje;

9.3.2 úplný a aktuální zdrojový kód tam, kde je to s ohledem na plnění Smlouvy smysluplné;

9.3.3 seznam platných administrátorských účtů Dodavatele k produkční instanci IS IPPC a platných hesel k nim;

9.3.4 úplnou knowledge base týkající se poskytování služeb, pokud bylo předmětem poskytování průběžně poskytovaných služeb, vč. popisu a seznamu uzavřených a neuzavřených servisních požadavků;

9.3.5 aktuální seznam standardních provozních úkonů pro údržbu aktiv Objednatele;

9.3.6 případně veškeré další informace, data, dokumenty nebo údaje, o které Objednatel Dodavatele požádá.

10. ŘÍZENÍ KONTINUITY ČINNOSTÍ

10.1 Dodavatel se ve vztahu k poskytování plnění dle Smlouvy zavazuje zavést a udržovat vhodná opatření pro zajištění kontinuity činností vč. opatření blíže stanovených v Pravidlech pro dodavatele a bezpečnostních politikách. Zejména se Dodavatel zavazuje:

10.1.1 zajistit adekvátní kontinuitu aktiv, která jsou potřebná k poskytování plnění dle Smlouvy; a

10.1.2 pravidelně kontrolovat a testovat, že je Dodavatel schopen zajistit kontinuitu aktiv při dodržení sjednané úrovně plnění dle Smlouvy.

10.2 Dodavatel se zavazuje poskytnout nezbytnou součinnost při zpracování a testování plánů obnovy a havarijních plánů a plnění dalších povinností Objednatele dle § 15 VKB.

11. PŘEDÁNÍ DAT, ÚDAJŮ A INFORMACÍ

11.1 Dodavatel se zavazuje na základě výzvy Objednatele a při ukončení Smlouvy, bez zbytečného odkladu předat Objednateli bezpečným způsobem, ve strojově čitelné podobě a ve formátu zaručujícím kompatibilitu v procesu migrace jakákoli jemu předaná Objednatelem či jiným způsobem získaná nebo vytvořená data při plnění Smlouvy (dále jen „Data“) a Důvěrné informace v dispoziční sféře Dodavatele. Dodavatel se k výzvě Objednatele zavazuje poskytnout nezbytnou součinnost, přičemž si Smluvní strany mohou písemně dohodnout jiný způsob předání Dat a Důvěrných informací. Dodavatel je povinen i bez výzvy Objednatele předat Objednateli Data do 7 dnů po skončení účinnosti Smlouvy.

12. LIKVIDACE DAT

12.1 Dodavatel se zavazuje při ukončení účinnosti Smlouvy, případně na písemnou žádost Objednatele, bez zbytečného odkladu po předání Dat a Důvěrných informací, nejpozději však do 14 dnů, zlikvidovat Data a Důvěrné informace v souladu s Pravidly dodavatele a bezpečnostními politikami za podpůrného užití přílohy č. 4 VKB, to vše za možného dozoru zástupce Objednatele.

12.2 V případě, že má Dodavatel na svých nosičích Data vysoké či kritické úrovně dle přílohy č. 1 VKB (úroveň Chráněné ve smyslu Pravidel pro dodavatele a bezpečnostních politik), má povinnost tato Data ve lhůtě podle odst. 12.1 zlikvidovat protokolárně. Dodavatel o takové likvidací poskytne Objednateli, a to i bez vyžádání, písemnou zprávu.

13. ODSTOUPENÍ OD SMLOUVY

13.1 Objednatel je oprávněn jednostranně odstoupit od Smlouvy v případě:

13.1.1 podstatného porušení práv a povinností dle této Přílohy Dodavatelem; a/nebo

13.1.2 opakovaného (nejméně třikrát) porušení práv a povinností dle této Přílohy Dodavatelem.

13.2 Dodavatel je dále oprávněn odstoupit od Smlouvy, pokud dojde k významné změně kontroly nad Dodavatelem, přičemž kontrolou se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2020 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení nebo dojde ke změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k plnění Smlouvy a tato změna bude Objednatelem vyhodnocena jako bezpečnostní riziko ve smyslu ZKB a/nebo VKB.

14. SANKCE ZA PORUŠENÍ POVINNOSTÍ

14.1 V případě porušení jakékoli povinnosti Dodavatele dle této Přílohy, je Objednatel oprávněn požadovat smluvní pokuty, jak jsou vymezeny níže, a to za každé jednotlivé porušení, nestanoví-li Smlouva za takové porušení smluvní pokutu vyšší. Objednatel je oprávněn požadovat pokuty v případě, že:

14.1.1 došlo k porušení této Přílohy Dodavatelem, a to ve výši 10.000,- Kč (deset tisíc korun českých);

14.1.2 došlo k porušení této Přílohy Dodavatelem, přičemž toto porušení vedlo ke kybernetickému bezpečnostnímu incidentu, a to ve výši 30.000,- Kč (třicet tisíc korun českých);

14.1.3 porušení této Přílohy Dodavatelem vážně ohrožující bezpečnost informací ve vztahu k aktivům Objednatele trvá navzdory písemné výzvě Objednatele pod dobu delší 3 dnů, a to ve výši 50.000,- Kč (padesát tisíc korun českých) za každý započatý den.

14.2 Smluvní pokutou není dotčeno právo Objednatele požadovat náhradu škody ve výši převyšující zaplacenou smluvní pokutu.

15. ZÁVĚREČNÁ UJEDNÁNÍ

15.1 Dodavatel se zavazuje při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahujících se k pravidlům bezpečnosti, jejichž následkem může vzniknout újma nebo nesoulad s právními předpisy a zajistit ve spolupráci se Objednatelem náhradní způsob naplnění pravidel bezpečnosti, pokud stávající řešení přestalo být funkční nebo efektivní.

15.2 Pokud není ve Smlouvě nebo v této Příloze uvedeno jinak, odměna za provádění opatření dle této Přílohy je součástí odměny dle Smlouvy.

PŘÍLOHA Č. 2

PRAVIDLA PRO DODAVATELE A BEZPEČNOSTNÍ POLITIKY

KOMUNIKACE

Dodavatel má povinnost komunikovat s osobami oprávněnými a určenými ve smlouvě (dále jen zástupci MŽP) nejen v rámci smluvního vztahu, ale také v oblastech týkajících se bezpečnosti jím dodaného, příp. jím provozovaného informačního systému.

Dodavatel se podílí na vytvoření a aktualizaci analýzy rizik vztahující se k jím dodanému/provozovanému informačnímu systému.

Jedná-li se o dodavatele, jehož systém nějakým způsobem navazuje na další informační systémy MŽP, bude dodavatel upozorněn, že má povinnost účastnit se pravidelných integračních schůzek, aby bylo zajištěno správné fungování těchto propojení.

ŘÍZENÍ INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI

Dodavatel má povinnost ve svých interních procesech realizovat tato opatření:

- ***má zaveden ISMS v rozsahu minimálně pokrývajícím předmět smluvního vztahu***
- ***má stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí v následující formě, obsahu a rozsahu:***
  - ***poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;***
  - ***potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;***
- ***má určeny osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;***
- ***v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;***
- ***pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelná odborná školení, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti;***
- ***v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;***
- ***zajišťuje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a má nastaven proces disciplinárního řízení pro své zaměstnance;***

- ***v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajišťuje předání odpovědností;***
- ***hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí;***
- ***určuje pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;***
- ***vede o provedených školeních přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.***
- ***alespoň jedenkrát ročně předává MŽP informace, týkající se osob souvisejících s poskytovaným předmětem plnění smlouvy, o provedených školeních a jejich obsahu.***

Využívá-li dodavatel při poskytování předmětu plnění poddodavatele, je povinen zajistit adekvátní dodržování těchto bezpečnostních pravidel rovněž ve smluvních vztazích se svými poddodavateli.

Zástupci MŽP si vyhrazují právo vést záznamy a prověřovat činnosti dodavatele, vést záznamy o incidentech a nestandardních činnostech zaměstnanců a dalších osob působících ve prospěch dodavatele (dále jen „zaměstnanci dodavatele“). Na základě těchto záznamů má oprávnění vyhodnocovat důvěryhodnost a spolehlivost zaměstnanců dodavatele. V případě identifikovaného rizika oznámí MŽP nesoulad dodavateli a obě strany vejdou v jednání pro řešení této situace.

PERSONÁLNÍ BEZPEČNOST

Dodavatel zajistí prokazatelné seznámení všech osob, účastnících se plnění dle uzavřené smlouvy s MŽP s těmito bezpečnostními pravidly a dalšími upřesňujícími bezpečnostními informacemi prokazatelně předanými ze strany MŽP.

Osoby, účastnící se plnění dle uzavřené smlouvy s MŽP musí mít prokazatelné potřebné kvalifikační předpoklady, zkušenosti a znalosti.

Dodavatel musí zajistit, aby osoby, účastnící se plnění dle uzavřené smlouvy s MŽP prošly procesem prověřování a byly jim stanoveny pro jejich činnosti podmínky a odpovědnosti.

FYZICKÁ BEZPEČNOST, POŽÁRNÍ OCHRANA A BOZP

Podmínky a pravidla fyzické bezpečnosti, požární ochrany a bezpečnosti a ochrany zdraví při práci jsou popsány ve smlouvě s MŽP.

ŘÍZENÍ PROVOZU

Dodavatel se zavazuje:

- ***zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění v souladu s požadavky 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 „VoKB“) a doporučeními technických norem řady ISO/IEC 27000;***
- ***na vyžádání poskytnout MŽP přehled o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře, kterými plní předmět smlouvy.***

ŘÍZENÍ PŘÍSTUPU

Identifikace

- ***Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele, musí mít v rámci své ICT infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role, pokud to architektura informačního systému vyžaduje. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji.***
- ***Každý zaměstnanec dodavatele, pokud přistupuje k interním informačním systémům MŽP, má u MŽP veden a evidován jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu smlouvy.***

Autentizace

Podmínky pro autentizaci při využití ICT infrastruktury MŽP:

- ***k jednoznačné identifikaci privilegovaných uživatelů systémů se využívá více faktorová autentizace;***
- ***ověření heslem - pokud není možné použít jednoznačnou identifikaci privilegovaných uživatelů více faktory, je použita autentizace pomocí kryptografických klíčů se zaručením obdobné úrovně bezpečnosti nebo použití hesla s definovanými pravidly.***

Autorizace

- ***Zaměstnanci dodavatele jsou povinni v ICT infrastruktuře MŽP využívat privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy. Uživatelé nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou informačního systému.***
- ***Zaměstnanci dodavatele jsou informováni MŽP, které informace MŽP***

považuje za chráněné, ke kterým chráněným informacím MŽP mají přístup, a jak s nimi mohou nakládat, a to vždy, kdy má k předání informací dojít. Jakékoliv manipulace a další operace s chráněnými informacemi MŽP, které nebyly výslovně v instrukcích uvedeny, nemá dodavatel povoleny.

Vzdálený přístup

Pracovní stanice dodavatele přistupující k infrastruktuře MŽP prostřednictvím VPN (Virtual Private Network) musí mít:

- ***pokročilou funkční antivirovou ochranu (s real time protection mod), s pečetí AV-TEST APPROVED (av-test.org) nebo s certifikátem VB100 (virusbulletin.com) – platí pro prostředí MS Windows a Android;***
- ***funkční personal firewall;***
- ***funkční nastavené automatické aktualizace systému;***
- ***operační systém, který není mimo servisní podporu výrobce (pokud není smluvním ujednáním výslovně stanoveno jinak);***
- ***aktualizované aplikace třetích stran za dodržení autorských práv třetích stran;***
- ***zajištěno šifrování všech paměťových médií, na kterých jsou uložena chráněná data a informace MŽP. Přístup k paměťovým médiím a k dešifrování chráněných dat a informací MŽP musí být umožněno jen oprávněným osobám dodavatele;***
- ***nainstalovaného VPN klienta, instalovaného výlučně v odpovědnosti dodavatele;***
- ***druhý autentizační faktor (HW nebo SMS token) pro přístup k VPN, který bude poskytnut určeným zaměstnancem MŽP proti podpisu předávacího protokolu.***

MŽP může nařídit dodavateli přístup ke svým zdrojům prostřednictvím systému PIM/PAM (Privileged Identity Management/Privileged Access Management).

SPRÁVA A NAKLÁDÁNÍ S PŘIHLAŠOVACÍMI ÚDAJI

Tvorba přihlašovacích údajů

V případě, že dodavatel vytváří uživatelské nebo jiné účty v rámci jím spravované nebo provozované aplikace, musí být hesla vytvořena minimálně v souladu s požadavky definovanými ve vyhlášce o kybernetické bezpečnosti.

Práce s přihlašovacími údaji

S přihlašovacími údaji musí být v rámci organizace dodavatele nakládáno v souladu s požadavky ve vyhlášce o kybernetické bezpečnosti.

Pokud dodavatel obdrží od MŽP přihlašovací údaje:

a) musí udržovat tyto údaje v tajnosti
b) v případě vyzrazení nebo podezření na vyzrazení je neprodleně zneplatnit, změnit nebo zažádat MŽP o změnu,
c) v případě obdržení iniciačního hesla musí při prvním přihlášení toto heslo okamžitě změnit,
d) nesmí přihlašovací údaje sdílet s jinými osobami,
e) nesmí přihlašovací údaje ukládat v nezabezpečené podobě a nesmí je ukládat na místa snadno dostupná jiným osobám,
f) musí přihlašovací údaje ukládat ve formě odolné proti offline útokům,
g) v případě odchodu zaměstnance nebo nepotřebnosti účtu dané přihlašovací údaje okamžitě zneplatnit nebo o zneplatnění zažádat MŽP.

V případě předávání přihlašovacích údajů musí být tyto údaje předávány:

a) v zabezpečené (šifrované) formě odolné proti offline útokům,
b) prostřednictvím jiných komunikačních kanálů (uživatelské jméno odděleně od hesla).

ŘÍZENÍ ZMĚN

Podmínky:

- ***změny na straně dodavatele musí být řízeny s ohledem na kritičnost informací, systémů, procesů a opětovným posuzováním rizik.***

Dodavatel se zavazuje:

- ***řídit a evidovat smluvní změny;***
- ***řídit a evidovat změny v poskytovaných službách v souladu s požadavky VoKB a doporučeními technických norem řady ISO/IEC 27000.***

AKVIZICE, VÝVOJ A ÚDRŽBA

Dodavatel se zavazuje:

- ***zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění;***

V případě vývoje řešení se dodavatel zavazuje:

- ***dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru dle doporučení technických norem řady ISO/IEC 27000;***
- ***pokud jsou softwarové auditní činnosti a předání zdrojového kódu k řešení součástí plnění dle smlouvy, bude umožněn audit prováděného nebo provedeného plnění a na písemnou žádost bude předložen vyvíjený zdrojový kód k řešení na provedení code review (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), a to zejména za účelem ověření skutečnosti, zda bylo postupováno dle plnění v souladu se smlouvou;***
- ***zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování řešení a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že řešení nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.);***
- ***pokud je součástí plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí MŽP;***
- ***zajistit bezpečnost testovacího prostředí u dodavatele, pokud je zřízeno, a ochranu poskytnutých testovacích dat MŽP;***
- ***zajistit, že v produkčním prostředí MŽP bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění;***
- ***zajistit, že v rámci poskytovaného plnění bude dodávané řešení v souladu s doporučeními technických norem řady ISO/IEC 27000;***
- ***poskytnout MŽP potřebnou součinnost v případě, že MŽP vyžaduje / realizuje provedení bezpečnostních testů (např. penetračních testů) souvisejících s předmětem plnění;***
- ***předat zdrojový kód MŽP, je-li tak stanoveno ve smlouvě, bezpečnou formou zajišťující jeho integritu, a v takovém případě:***
    - zajistit řízení verzí zdrojového kódu;
    - zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí;
    - zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů;
- nevyvíjet, nekompilovat a nešířit v prostředí MŽP programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

Je-li v rámci předmětu plnění vyžadováno použití kryptografických prostředků, technické podmínky jsou následující:

- ***šifrování symetrickým heslem nejméně metodou AES 256. Heslo musí být předáno jiným komunikačním kanálem;***
- ***šifrování pomocí digitálních certifikátů vydaných obecně uznávanou CA***

nebo CA, které explicitně důvěřují obě strany;

- ***pokud nelze ověřit platnost certifikátu vůči CRL, je certifikát považován za neplatný a nelze jej použít k šifrování nebo podpisu;***
- ***šifrování pomocí PGP klíčů odsouhlasených oběma stranami nebo ověřené nezávislou důvěryhodnou třetí stranou;***
- ***pro VPN přístup se používá šifra AES256/SHA256 nebo silnější;***
- ***pro webové servery používají HTTPS protokol minimálně se šifrou TLS 1.2;***

MONITORING

Přístup zaměstnanců dodavatele k vybraným chráněným interním informacím a k informačním a komunikačním systémům MŽP je nepřetržitě zaznamenáván, monitorován a vyhodnocován. Události v systémech jsou MŽP zaznamenávány do logů:

- ***úspěšné a neúspěšné přihlášení a odhlášení uživatelů;***
- ***činnosti provedené administrátory;***
- ***úspěšné a neúspěšné manipulace s účty, oprávněními a právy;***
- ***neprovedení činností v důsledku nedostatku přístupových oprávnění;***
- ***činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;***
- ***zahájení a ukončení činností technických aktiv;***
- ***automatická varovná nebo chybová hlášení technických aktiv;***
- ***přístupy k logům, pokusy o manipulaci s logy a změny nastavení nástroje pro zaznamenávání činností a použití mechanismů autentizace včetně změny údajů, které slouží k přihlášení.***

Dodavatel je povinen průběžně monitorovat v rámci své ICT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty atd.

OCHRANA DATOVÝCH ÚLOŽIŠŤ A PŘENOSNÝCH MÉDIÍ

Uložení chráněných informací MŽP do datových úložišť, na přenosná média a případný transport médií mimo prostory MŽP podléhá schválení MŽP.

V případě ukládání chráněných informací MŽP do datových úložišť a na přenosná média má dodavatel povinnost ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a vést evidenci těchto médií.

Dodavatel je povinen zajistit likvidaci operativních dat MŽP ihned po pominutí účelu jejich zpracování nebo uložení způsobem dle standardu NIST 800-88. Po likvidaci dat na elektronickém

médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí dodavatel vést protokol.

KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY

Dodavatel má za povinnost hlásit veškerá podezření na kybernetické bezpečnostní události:

- ***odpovědné osobě MŽP v termínu bezprostředně (bez prodlení) po zjištění kybernetické bezpečnostní události / incidentu;***
- ***prostřednictvím emailu, telefonicky se zajištěním evidence hovoru na obou stranách, nebo osobně;***
- ***s popisem:***
    - data a času zjištění;
    - povahy události;
    - zdroje události;
    - cíle / oběti události;
    - potencionálního dopadu.

V případě, že je dodavatel současně i provozovatelem (jedním z provozovatelů) systému, má k systému povinnosti ze ZoKB. Některé z povinností jsou mimo jiné hlásit kontaktní údaje a hlásit kybernetické bezpečnostní incidenty prostřednictvím formuláře na webových stránkách NÚKIB přímo Národnímu úřadu pro kybernetickou a informační bezpečnost.

AUDIT DODAVATELE (ZÁKAZNICKÝ AUDIT)

Oprávnění k provedení auditu dodavatele v případě odůvodněné potřeby:

- ***MŽP si vyhrazuje právo provádět audity dodavatele.***
- ***MŽP s dostatečným předstihem alespoň 5 pracovních dnů oznámí dodavateli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že MŽP se zavazuje postupovat tak, aby nenarušil provozní potřeby dodavatele.***
- ***MŽP si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování dodavatele) v souvislosti s plněním smlouvy provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.***
- ***Dokumentace auditů prováděných MŽP je vedena v útvaru odpovědném za provádění auditu. 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).

Auditovaná strana (dodavatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění, na jejichž základě:

- ***dodavatel navrhne opatření a termíny řešení a předá jejich seznam MŽP k odsouhlasení.***
- ***MŽP následně potvrdí souhlas s navrženými opatřeními nebo je vrátí s připomínkami dodavateli k přepracování.***

Nápravná opatření

- ***Auditovaná strana (dodavatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření.***
- ***Zprávu o realizovaných opatřeních dodavatel oznamuje a předává MŽP***

PENETRAČNÍ TESTOVÁNÍ

Dodavatel se zavazuje poskytnout MŽP potřebnou součinnost v případě, že MŽP vyžaduje / realizuje provedení bezpečnostních testů (např. penetračních testů) souvisejících s předmětem plnění.

Z průběhu penetračního testování bude sepsána závěrečná zpráva, ve které budou uvedeny nalezené neshody a doporučení. Na realizaci případných nápravných opatření vyplývající z provedeného penetračního testu se domluví MŽP s dodavatelem. V návaznosti na nálezech bude nutné ze strany dodavatele v určeném čase zajistit bez/úplatně (dle konkrétních nálezů) realizaci dohodnutých nápravných opatření.

Zprávu o realizovaných opatřeních dodavatel oznamuje a předává MŽP.

OCHRANA AKTIV PROTI NEAUTORIZOVANÝM ČINNOSTEM

Dodavatel na aktiva MŽP neinstaluje a nepoužívá nástroje, které nejsou součástí předmětu plnění.

PODMÍNKY PŘI UKONČENÍ SMLOUVY

V případě ukončení smluvního vztahu musí být ukončeny veškeré přístupy dodavatele a jeho zaměstnanců k aktivům MŽP nejpozději k termínu ukončení smluvního vztahu.
Pokud byla zaměstnancům dodavatele poskytnuta aktiva MŽP, musí být tato aktiva vrácena nejpozději k termínu ukončení smluvního vztahu.
Pokud byla dodavateli poskytnuta informační aktiva (data) MŽP, musí být nejpozději k termínu ukončení smluvního vztahu vrácena a beze zbytku smazána způsobem dle standardu NIST 800-88 ze všech ***informačních*** systémů dodavatele a nosičů dodavatele taková aktiva obsahujících (není-li ve smlouvě uvedeno jinak).