

PŘÍLOHA Č. 4

SMLOUVY O NÁVRHU, VÝVOJI, IMPLEMENTACI A SPRÁVĚ INFORMAČNÍHO SYSTÉMU
 PORTÁL SLUŽEB SFDI

KYBERNETICKÁ BEZPEČNOST



# ÚVODNÍ USTANOVENÍ

## Z důvodu nutnosti plnění povinností stanovených Objednateli jakožto povinné osobě ve smyslu Vyhlášky o kybernetické bezpečnosti je Poskytovatel povinen nad rámec povinností stanovených Smlouvou plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této Přílohy č. 4 Smlouvy. Účelem této Přílohy č. 4 Smlouvy tak je dodržet povinnost Objednatele dle § 4 odst. 4 ZKB zahrnout požadavky vyplývající z bezpečnostních opatření do smluvního ujednání s Poskytovatelem.

## Poskytovatel je povinen plnit relevantní povinnosti v rozsahu a způsobem, aby byl naplněn účel 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 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 č. 4 Smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti Poskytovatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

# Systém řízení bezpečnosti informací

## Poskytovatel je povinen se v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 3 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### 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 dle Smlouvy.

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

### 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.

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

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

## Poskytovatel je dále povinen dodržovat bezpečnostní politiku Objednatele,  kterou obdrží k seznámení.

# Řízení aktiv

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 4 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### 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 Dnů od akceptace Analýzy a následně na vyžádání, a to po celou dobu trvání Smlouvy a do tří měsíců po jejím ukončení. Pokud se nedá stanovit, která aktiva jsou využita, je nutné rozsah a seznam aktiv stanovit a udržovat tak, aby nebylo žádné relevantní aktivum opomenuto.

# Řízení rizik

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 5 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění dle Smlouvy.

### V minimálním intervalu jednou ročně (nebo i v případě významných změn činností prováděných pro Objednatele nebo změn PORTÁLU SLUŽEB SFDI či jiných aktiv napojených na PORTÁL SLUŽEB SFDI) vytvořit a bude-li to Objednatel požadovat, předložit mu zprávu o hodnocení rizik, která bude minimálně pokrývat:

#### Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok;

#### Identifikaci a hodnocení rizik s vazbou na předmět plnění;

#### Realizovaná bezpečnostní opatření;

#### Nepokrytá bezpečnostní rizika a návrh opatření;

#### Vyhodnocení bezpečnostních událostí a incidentů;

#### Aktuální stav souladu Poskytovatele s Kybernetickými požadavky včetně přehledu Kybernetických požadavků, které:

#### nebyly aplikovány, včetně odůvodnění, a

#### byly aplikovány, včetně způsobu plnění.

# Organizační bezpečnost

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 6 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### Jmenovat nejpozději do třiceti (30) Dnů po uzavření Smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění Kybernetických požadavků a související komunikaci mezi Smluvními stranami („**Kontaktní osoba pro kybernetickou bezpečnost**“). Kontaktní osobu pro kybernetickou bezpečnost sdělí Poskytovatel písemně Objednateli v téže lhůtě.

### Využívat pro poskytování předmětu plnění dle Smlouvy pouze oprávněných osob, které byly řádně seznámeny s příslušnými ustanoveními interních předpisů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění dle Smlouvy a stanovit bezpečnostní role těchto oprávněných osob s jasně definovanými odpovědnostmi a pravomocemi.

# Řízení dodavatelů

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 8 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### Využívá-li při poskytování předmětu plnění dle Smlouvy Poddodavatele, zabezpečit v obdobném rozsahu dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými Poddodavateli.

### Dodržovat podmínky pro zapojení Dalšího zpracovatele při zpracování Osobních údajů.

# Bezpečnost lidských zdrojů

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 9 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### Zabezpečit, aby Kontaktní osoba pro kybernetickou bezpečnost nejpozději do šedesáti (60) Dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování předmětu plnění dle Smlouvy za Poskytovatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních předpisů Objednatele, existují-li takové.

### Dodržovat příslušná ustanovení interních předpisů Objednatele v rozsahu, v jakém byl s těmito akty 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.

### Při provádění dohledu nad předmětem plnění dle Smlouvy, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění dle Smlouvy.

### Zabezpečit, aby osoby podílející se na poskytování plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:

#### Pro uložení a sdíleni dat a informací Objednatele využívali pouze k tomu schválené prostředky (aktiva) a schválené způsoby komunikace;

#### Neukládali ani nesdíleli data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující dobré jméno Objednatele;

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

#### Nenavštěvovali internetové stránky s eticky nevhodným obsahem;

#### Nerealizovali pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;

#### 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;

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

#### Dodržovali obecně závazné právní předpisy

## Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele zpracování osobních údajů pověřených osob Poskytovatele, které se podílejí na poskytování plnění dle Smlouvy. Pokud nebude Objednateli umožněno osobní údaje pověřených osob Poskytovatele zpracovat, nebude těmto pověřeným osobám umožněn žádný přístup ke zdrojům Objednatele.

## Poskytovatel je dále povinen:

### Prohlubovat znalosti osob podílejících se na poskytování plnění Objednateli v oblasti bezpečnosti informací.

### Stanovit práva a povinnosti osob podílejících se na poskytování plnění Objednateli v oblasti bezpečnosti informací.

# Řízení provozu a komunikací

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 10 Vyhlášky kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

### Na vyžádání ve lhůtě, která nebude kratší než šest (6) 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.

### Zabezpečit, že pro poskytování předmětu plnění dle 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.

## Poskytovatel je dále povinen provést a zabezpečit dodržování následujících opatření:

### Implementaci procesů pro řízení ICT (tj. řízení incidentů, řízení změn, řízení životního cyklu systémů apod.).

### Zavedení postupů pro ochranu proti škodlivému kódu, řízení technických zranitelností v informačním systému, který je využíván k poskytování předmětu plnění dle Smlouvy.

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

### Stanovení pracovních postupů pro instalaci, spouštění, ukončování provozu technických aktiv, pracovní postupy pro řešení mimořádných stavů.

### Řízení přístupu k datům a systémům, které spadají do rozsahu poskytování předmětu plnění dle Smlouvy.

### Provádění pravidelného zálohování a kontroly použitelnosti provedených záloh dle požadavku Objednatele.

### Zavedení postupů pro sledování kybernetických bezpečnostních událostí a opatření pro ochranu přístupu k záznamům o těchto událostech.

# Řízení změn

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 11 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

### Aktivně spolupracovat při testování významné změny v oblasti kybernetické bezpečnosti na straně Objednatele.

# Řízení přístupu

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 12 Vyhlášky kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.

### 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 účinnosti této Smlouvy a tři měsíce po jejím ukončení ve lhůtě, která nebude kratší než šest (6) Pracovních dnů, ledaže bude příslušným orgánem veřejné moci požadováno jinak.

### Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT Objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 Den).

### Zabezpečit, aby osoby podílející se na poskytování předmětu plnění dle Smlouvy a mající přístup k informačním aktivům Objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.

### Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do prostředí Objednatele.

## Poskytovatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Poskytovatele/Poddodavatele, a to na základě požadavku Poskytovatele na přístup.

## Poskytovatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.

## Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele 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).

## Poskytovatel je dále povinen omezit přidělování administrátorských oprávnění.

# Akvizice, vývoj a údržba

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 13 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### Zabezpečit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění dle Smlouvy.

### Předat Objednateli dokumentaci předmětu plnění dle Smlouvy nad rámec rozsahu stanoveného ve Smlouvě minimálně v následujícím rozsahu:

#### dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;

#### dokumentaci obsahující popis autorizačního konceptu a oprávnění;

#### dokumentaci obsahující instalační a konfigurační postupy.

Výše uvedenou dokumentaci, není-li již zahrnuta v Dokumentaci, Poskytovatel předá Objednateli v přiměřené lhůtě dle dohody Smluvních stran.

## V případě, že předmět plnění dle Smlouvy zahrnuje vývoj Softwaru, je Poskytovatel povinen:

### Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj Softwaru.

### Na vyžádání alespoň šest Pracovních dnů předem, nepožaduje-li příslušný orgán veřejné moci jinak, umožnit Objednateli provedení auditu prováděného nebo provedeného plnění a na vyžádání předložit Objednateli vyvíjený Zdrojový kód na provedení codereview, a to zejména za účelem ověření skutečnosti, zda Poskytovatel postupuje či postupoval při poskytování plnění v souladu se Smlouvou a Kybernetickými požadavky. S ohledem na faktické a časové podmínky Smlouvy se Smluvní strany dohodly, že Objednatel bude oprávněn využít tohoto práva nejdříve od zahájení testovacího provozu dle Harmonogramu.

### Poskytovat Objednateli v termínech stanovených Objednatelem, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje Softwaru (nejdříve od zahájení testovacího provozu dle Harmonogramu) či kdykoli po jeho předání.

### Zabezpečit, že plnění dle Smlouvy bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve Smlouvě (zejména, že Software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

### Pokud je součástí plnění dle 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 Testovacím prostředí či Produkčním prostředí.

### Zajistit bezpečnost Testovacího prostředí u Poskytovatele a ochranu poskytnutých testovacích dat Objednatelem.

### Zabezpečit, že do Produkčního prostředí bude dodán jen předmětem Smlouvy specifikovaný kompilovaný, respektive spustitelný Zdrojový kód a další nezbytná data pro provozování předmětu plnění dle Smlouvy.

### Zabezpečit, že v rámci poskytovaného plnění bude dodávaný Software

#### v souladu s bezpečnostními politikami a standardy Objednatele; a

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

### Instalovat Software pouze na základě Objednatelem předem schválených migračních postupů.

### Předat Zdrojový kód Objednateli bezpečnou formou zajištující jeho integritu.

### Zabezpečit řízení verzí Zdrojového kódu.

### Zabezpečit zálohování Zdrojového kódu a jeho uložení mimo Produkční prostředí.

### Zabezpečit, aby distribuce Zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto Zdrojových kódů.

### 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.

# Zvládání kybernetických bezpečnostních událostí a incidentů

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 14 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

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

### Vyhodnocovat informace o kybernetických bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky použitelné platné a účinné legislativy.

### 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 Poskytovatele.

### 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 analýze příčin kybernetického bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Poskytovatel kybernetický bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

## Poskytovatel bere na vědomí, že postup zvládání kybernetického bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující odpovědnost 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 ve Smlouvě nejsou tímto ustanovením dotčena.

# Řízení kontinuity činností

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 15 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

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

### Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle sjednané SLA.

# Kontrola a audit

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Národního úřadu pro kybernetickou a informační bezpečnost dle § 23 ZKB.

## Poskytovatel umožní Objednateli alespoň jednou ročně po dobu účinnosti Smlouvy a pak jeden (1) rok po ukončení Smlouvy provedení auditu kybernetické bezpečnosti u Poskytovatele a jeho Poddodavatelů:

### jehož rozsah bude ohraničen využíváním ICT prostředků Poskytovatele pro potřeby plnění Smlouvy a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Poskytovatele a

### jehož předmětem bude naplnění Kybernetických požadavků a vyhodnocení rizik dle bodu 4 této Přílohy č. 4 Smlouvy.

## Objednatel je oprávněn při auditu kybernetické bezpečnosti využít třetí stranu. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by audit kybernetické bezpečnosti prováděl sám, včetně odpovědnosti za způsobenou újmu.

## Poskytovatel umožní Objednateli audit kybernetické bezpečnosti provedený prostředky Objednatele nebo třetí strany, a to v lokalitě Poskytovatele i vzdáleně, pokud to technické prostředky Poskytovatele umožňují.

## Poskytovatel je povinen odstranit nedostatky zjištěné:

### na základě provedení hodnocení rizik dle bodu 4 v této Příloze č. 4 Smlouvy; nebo

### v rámci auditu kybernetické bezpečnosti dle bodu 14.2 této Přílohy č. 4 Smlouvy;

## odstranit ve lhůtě určené v písemném oznámení Objednatele, která nebude kratší než dvacet (20) Pracovních dnů. Nestanoví-li Objednatel lhůtu v písemném oznámení, zavazují se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší devadesát (90) Dnů.

## Poskytovatel je dále povinen:

### Poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků.

### Na požádání s Objednatelem konzultovat kdykoli v průběhu realizace plnění dle Smlouvy detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků a pro takovéto konzultace zajistit účast kvalifikovaných pracovníků.

### Neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků, které nastanou kdykoli v průběhu trvání této Smlouvy.

### Bezodkladně a s vyvinutím nejlepšího úsilí zajistit náhradní způsob naplnění Kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní.

### Při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům, jejichž následkem může vzniknout újma nebo nesoulad se zákony nebo jinými obecně závaznými právními předpisy.

# Technická opatření

## Poskytovatel se bude v rozsahu předmětu plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 17 až § 27 Vyhlášky o kybernetické bezpečnosti, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu plnění dle Smlouvy na své straně:

### Dodržovat interní předpisy Objednatele a 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.

### V rozsahu předmětu plnění dle 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.

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

### Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) s využitím dvoufaktorové autentizace.

### Připojovat do 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.

### 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 Poskytovatele.

### Na aktiva Objednatele bez jeho písemného souhlasu neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu plnění dle Smlouvy:

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

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

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

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

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

### Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru a která jsou v souladu s interními předpisy Objednatele.

### 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.

### Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění dle Smlouvy, a to po celou dobu trvání Smlouvy a pak po dobu dvou (2) let po jejím ukončení.

### Zabezpečit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění dle Smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

### Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.

### Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

## 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.

## 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 dokumenty Objednatele, se kterými byl Poskytovatel seznámen.

# Další povinnosti Smluvních stran v oblasti kybernetické bezpečnosti

## S ohledem na to, že Poskytovatel je významným dodavatelem a provozovatelem ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 Vyhlášky o kybernetické bezpečnosti, je Objednatel povinen do smluvního ujednání s Poskytovatelem začlenit úpravu relevantních oblastí dle přílohy č. 7 k Vyhlášce o kybernetické bezpečnosti.

## Smluvní strany uvádějí, že:

#### ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity) upravuje zejména čl. 12 Smlouvy,

#### ustanovení o oprávnění užívat data upravuje zejména čl. 10 Smlouvy,

#### ustanovení o autorství programového kódu, popřípadě o programových licencích upravuje zejména čl. 10 Smlouvy,

#### ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu) upravuje zejména bod 14 této Přílohy č. 4 Smlouvy,

#### ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že Poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi Objednatelem a Poskytovatelem a nebudou v rozporu s požadavky Objednatele na dodavatele, upravuje bod 6 této Přílohy č. 4 Smlouvy.

#### ustanovení o povinnosti Poskytovatele dodržovat bezpečnostní politiky Objednatele nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou upravuje bod 2.2 této Přílohy č. 4 Smlouvy,

#### ustanovení o řízení změn upravuje zejména čl. 7 Smlouvy,

#### ustanovení o souladu Smlouvy s obecně závaznými právními předpisy upravuje zejména odst. 3.6 Smlouvy, čl. 13 Smlouvy a čl. 14 Smlouvy,

#### ustanovení o povinnosti Poskytovatele informovat Objednatele o

#### kybernetických bezpečnostních incidentech souvisejících s plněním Smlouvy upravuje zejména bod 12 této Přílohy č. 4 Smlouvy,

#### způsobu řízení rizik na straně Poskytovatele a o zbytkových rizicích souvisejících s plněním Smlouvy upravuje zejména bod 4 této Přílohy č. 4 Smlouvy,

#### Změně kontroly Poskytovatele upravuje zejména odst. 8.16 Smlouvy,

#### specifikace podmínek z pohledu bezpečnosti při ukončení Smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně) upravuje zejména čl. 18 Smlouvy,

#### specifikace podmínek pro řízení kontinuity činností v souvislosti s Poskytovatelem a Poddodavateli (například jejich zahrnutí do havarijních plánů, jejich úkoly při aktivaci řízení kontinuity činností) upravuje zejména odst. 18.8 a násl. Smlouvy,

#### specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání Objednatelem upravuje zejména čl. 11 Smlouvy a odst. 18.16 Smlouvy,

#### pravidla pro likvidaci dat upravuje zejména Příloha č. 3 Smlouvy a odst. 18.15 Smlouvy,

#### ustanovení o právu jednostranně odstoupit (resp. vypovědět bez výpovědní doby) od Smlouvy v případě Změny kontroly Poskytovatele upravuje zejména odst. 18.5 Smlouvy, a

#### ustanovení o sankcích za porušení povinností upravuje zejména čl. 16 Smlouvy.