BEZPEČNOSTNÍ STANDARDY

ČÁST I: Úvodní ustanovení a definice

1. Účel a předmět úpravy

Tato příloha (dále jen „Příloha“) stanovuje závazná bezpečnostní opatření (dále jen „Bezpečnostní opatření“), která Dodavatel dodržuje při poskytování plnění dle Smlouvy, jejíž nedílnou součást Příloha tvoří.

Opatření jsou definována s ohledem na skutečnost, že Objednatel podléhá rozsáhlým regulatorním povinnostem. Jako poskytovatel regulovaných služeb se řídí zákonem č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „Zákon o kybernetické bezpečnosti“) a současně, jakožto organizace působící v odvětví civilního letectví, naplňuje požadavky evropských nařízení s přímým dopadem na bezpečnost letectví.

Cíl Bezpečnostních opatření spočívá v zajištění ochrany důvěrnosti, integrity, dostupnosti, autenticity a odolnosti informací, informačních, komunikačních a průmyslových systémů a služeb Objednatele.

Dodavatel je povinen zavést a po celou dobu trvání smluvního vztahu udržovat přiměřená technická a organizační opatření v oblasti kybernetické bezpečnosti odpovídající povaze, rozsahu a rizikovosti poskytovaného plnění.

Dodavatel je povinen plnit tyto povinnosti v souladu s požadavky zákona č. 264/2025 Sb., o kybernetické bezpečnosti, a souvisejících prováděcích právních předpisů, případně, jde-li o dodavatele usazeného mimo Českou republiku, v souladu s právními předpisy provádějícími směrnici (EU) 2022/2555 (NIS2) v jeho domovském státě, v rozsahu odpovídajícím povaze poskytovaného plnění.

Splnění této povinnosti může Dodavatel prokázat zejména prostřednictvím platné certifikace systému řízení bezpečnosti informací, nezávislého bezpečnostního auditu, posouzení shody nebo jiného rovnocenného doložení.

2. Legislativní rámec

Bezpečnostní opatření a požadavky stanovené v této Příloze vycházejí z právních východisek a relevantních právních předpisů České republiky a Evropské unie, kterým Objednatel jakožto regulovaný subjekt podléhá. Objednatel na základě těchto předpisů sestavuje své bezpečnostní požadavky, které promítá do této Přílohy.

Dodavatel je povinen dodržovat veškerá bezpečnostní opatření a povinnosti stanovené v této Příloze, čímž Objednateli umožní dostát jeho regulatorním povinnostem.

Níže uvedené předpisy představují klíčová právní východiska, ze kterých požadavky Objednatele vycházejí:

a) Zákon o kybernetické bezpečnosti č. 264/2025 Sb., zejména ustanovení § 13 odst. 5, které ukládá povinnost zahrnout požadavky vyplývající z bezpečnostních opatření do smluv s dodavateli.

b) Prováděcí právní předpisy k Zákonu, zejména vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinnost (dále jen „Vyhláška“).

c) Nařízení Komise v přenesené pravomoci (EU) 2022/1645 ze dne 14. července 2022, kterým se stanoví požadavky na řízení rizik bezpečnosti informací s potenciálním dopadem na bezpečnost

letectví.

d) Prováděcí nařízení Komise (EU) 2015/1998 ze dne 5. listopadu 2015, kterým se stanoví prováděcí opatření ke společným základním normám letecké bezpečnosti.

e) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „GDPR“) a zákon č. 110/2019 Sb., o zpracování osobních údajů, v platném znění, pokud Dodavatel při plnění Smlouvy zpracovává osobní údaje pro Objednatele.

f) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

g) Nařízení Evropského parlamentu a Rady (EU) 2024/1689, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci.

h) Nařízení Evropského parlamentu a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828.

V případě, že se na určitou oblast vztahuje více právních předpisů, kterým Objednatel podléhá, jsou požadavky v této Příloze formulovány tak, aby poskytovaly nejvyšší úroveň bezpečnosti a ochrany. Tím se zajišťuje, že regulatorní komplexita nevede ke snížení bezpečnostní úrovně, ale naopak k jejímu posílení, což má pro Objednatele jako regulovaný subjekt zásadní význam.

3. Rozsah platnosti a aplikovatelnosti

Bezpečnostní opatření se uplatní vždy, když předmět plnění pro Objednatele (výhradně či jako součást jiného plnění) zahrnuje kteroukoli z následujících činností:

a) Vývoj, implementace, dodávka, poskytování, podpora nebo servis softwaru či hardwaru (dále jen „SW“ nebo „HW“).

b) Přístup Dodavatele do informačních, komunikačních anebo průmyslových systémů Objednatele, zejména těch, které byly určeny jako součást regulované služby ve smyslu Zákona o kybernetické bezpečnosti.

c) Zpracování, přenos, ukládání či archivace dat a provozních údajů Objednatele nebo jeho zákazníků (dále jen „Data Objednatele“).

Dodavatel posoudí, zda se jednotlivá opatření a povinnosti uvedené v Příloze vztahují přímo na něj, či na výrobce či poskytovatele jím dodávaného plnění. V návaznosti na výsledek posouzení zajistí Dodavatel jejich řádné plnění příslušnou osobou, přičemž vůči Objednateli nese plnou odpovědnost za splnění všech požadavků.

3.1 Specifika plnění

Dodavatel bere na vědomí, že předmět plnění Smlouvy, případně jeho dílčí části, podporují anebo spolupracují se systémy ve stanoveném rozsahu řízení kybernetické bezpečnosti Letiště Ostrava.

4. Definice pojmů

Pro účely Přílohy mají následující pojmy tento význam:

- Důvěrná informace: Veškeré informace, osobní údaje, data či zprávy, o nichž se Dodavatel dozvěděl v souvislosti s přípravou či plněním Smlouvy, a to včetně předmětu Smlouvy, skutečností tvořících obchodní tajemství a vnitřních záležitostí Objednatele.
- Kybernetický bezpečnostní incident: Narušení bezpečnosti informací v kybernetickém

prostoru, které má původ v kybernetickém prostoru a významný dopad na poskytování regulované služby. Pro účely Přílohy se za incident považuje jakákoli událost, která ohrožuje důvěrnost, integritu nebo dostupnost Dat Objednatele nebo systémů, v nichž se zpracovávají.

- Kybernetická bezpečnostní událost: Událost v kybernetickém prostoru, která by mohla vést ke vzniku kybernetického bezpečnostního incidentu.
- Poddodavatel: Jakákoli třetí strana, kterou Dodavatel zapojí do poskytování plnění dle Smlouvy.
- Zranitelnost: Slabé místo aktiva, které může zneužít jedna nebo více hrozeb.
- Klasifikace informací: Systém třídění informací Objednatele (např. Veřejné, Interní, Citlivé, Strategické), který určuje požadovanou míru jejich ochrany. Pokud Objednatel nestanoví jinak, Dodavatel nakládá se všemi Daty Objednatele a Důvěrnými informacemi minimálně jako s 'Interními'.

ČÁST II: Práva a povinnosti

5. Obecné povinnosti

5.1 Soulad s právními předpisy a politikami Objednatele

a) Dodavatel dodržuje příslušná ustanovení interních bezpečnostních politik, metodik a postupů Objednatele relevantních k předmětu plnění, pokud s nimi byl prokazatelně seznámen.

b) Objednatel se zavazuje poskytnout Dodavateli přístup k relevantní dokumentaci v nezbytném rozsahu.

c) Předmět plnění nesmí porušovat autorská práva a licenční podmínky třetích stran.

d) Objednavatel může předmět plnění nebo jeho části s náležitým odůvodněním odmítnout, pokud se na něj či na ně vztahují varování vydaná Národním úřadem pro informační a kybernetickou bezpečnosti.

5.2 Kontaktní osoba a odpovědnost

a) Nejpozději do 15 dnů po uzavření Smlouvy jmenuje Dodavatel zodpovědnou kontaktní osobu pro oblast kybernetické bezpečnosti a plnění povinností vyplývajících z Přílohy.

b) Kontaktní údaje této osoby sdělí Dodavatel Objednateli písemně ve stejné lhůtě.

c) Jakoukoli změnu kontaktní osoby Dodavatel nahlásí Objednateli do 5 pracovních dnů.

d) Nejpozději do 30 dnů od uzavření Smlouvy zajistí Dodavatel, aby jmenovaná kontaktní osoba písemně potvrdila Objednateli, že všechny osoby podílející se na poskytování plnění (včetně zaměstnanců Poddodavatelů) byly prokazatelně seznámeny s Objednatelem předloženou dokumentací a samotným obsahem Přílohy, přičemž se zavázaly k dodržování uvedených požadavků.

6. Informační povinnost

Dodavatel bez zbytečného odkladu písemně informuje Objednatele o následujících skutečnostech:

a) Jakákoli významná změna v ovládání Dodavatele podle zákona č. 90/2012 Sb., o obchodních korporacích.

b) Jakákoli změna vlastnictví základních aktiv, která se využívají k plnění předmětu Smlouvy.

c) Žádost cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána.

7. Personální bezpečnost a řízení přístupu

7.1 Požadavky na personál a seznámení s opatřeními

a) Dodavatel zajistí, aby všechny jeho osoby (zaměstnanci i externí spolupracovníci) a osoby jeho Poddodavatelů, které přicházejí do styku s Daty Objednatele nebo mají přístup do jeho systémů, vázala povinnost mlčenlivosti v rozsahu minimálně odpovídajícím závazkům stanoveným ve Smlouvě a této Příloze.

b) Dodavatel v souladu s požadavky a pokyny Objednatele zajistí poučení svých zaměstnanců a pracovníků třetích stran.

7.2 Prověření osob

a) Objednatel je oprávněn ověřit totožnost všech pracovníků Dodavatele a schválených subdodavatelů přistupujících k systémům Objednatele a jimi zpracovávaným údajům nebo službám. Výjimky z tohoto požadavku uděluje Objednatel pro konkrétní situace.

b) Dodavatel předává kontaktní údaje přistupujících pracovníků bez vyzvání.

7.3 Správa identit a řízení oprávnění

a) Dodavatel uplatňuje principy minimálního oprávnění (least privilege) a nezbytné znalosti (need-to-know).

b) Dodavatel přiděluje přístupová oprávnění k systémům a datům Objednatele na základě zdokumentované pracovní potřeby, pravidelně (minimálně jednou ročně) je reviduje a neprodleně odebírá po ukončení pracovního poměru, změně pracovní pozice nebo ukončení potřeby přístupu.

c) Dodavatel striktně oddělí uživatelské a administrátorské (privilegované) účty.

d) Pokud aplikace či systém, které jsou předmětem plnění, využívá technické, aplikační nebo databázové účty s ověřením pomocí hesla, musí u těchto účtů umožnit okamžitou a bezplatnou změnu hesla administrátorem na straně Objednatele.

7.4 Zabezpečení autentizace

a) Dodavatel nikdy neukládá přihlašovací údaje, zejména hesla, v čitelné podobě. Dodavatel je chrání pomocí dostatečně silných a aktuálních kryptografických prostředků v souladu s platnými doporučeními Národního úřadu pro kybernetickou a informační bezpečnost. Ta Dodavateli mohou být předána na vyžádání.

b) Pro veškerý vzdálený přístup do síťové infrastruktury Objednatele a pro veškerý přístup k rozhraním systémů spravujících Data Objednatele Dodavatel vynucuje použití vícefaktorové autentizace.

8. Bezpečnost v životním cyklu systémů a služeb

8.1 Bezpečný návrh a vývoj

a) Dodavatel prohlašuje a zaručuje, že veškerý jím dodávaný SW či HW byl vyvinut v souladu pravidly bezpečného vývoje.

b) Předmět plnění nesmí obsahovat žádné nepotřebné komponenty, služby, knihovny nebo uživatelské účty, které nejsou objektivně nutné pro jeho řádné fungování (princip minimalizace).

c) Dodavatel se zavazuje, že do předmětu plnění nebude úmyslně integrovat žádné zranitelnosti, zadní vrátka (backdoors), trojské koně, keyloggery, sniffery ani jinou formu škodlivého kódu a neučiní nic, co by takovou integraci umožnilo.

d) Na vyžádání Objednatele poskytne Dodavatel přesné informace o původu a skladbě

dodávaných komponent (Bill of Materials – BoM).

8.2 Řízení zranitelností a bezpečnostních aktualizací

a) Dodavatel průběžně sleduje a detekuje technické zranitelnosti a konfigurační nesoulady v předmětu plnění a jeho součástech třetích stran. O všech zjištěných skutečnostech, zejména o nově objevených zranitelnostech, bez zbytečného odkladu informuje Objednatele.

b) Dodavatel průběžně informuje Objednatele o vydávání bezpečnostních aktualizací (patchů) pro předmět plnění nebo jeho části.

c) Pokud součást plnění tvoří instalace operačního systému nebo SW třetích stran, Dodavatel je instaluje pouze v nejnovější stabilní verzi, plně podporované výrobcem.

d) Dodavatel odpovídá za to, že poskytované systémy v okamžiku předání obsahují nejnovější, stabilní a řádně odzkoušené bezpečnostní aktualizace.

8.3 Bezpečnostní testování a hodnocení

a) Objednatel si vyhrazuje právo kdykoli v průběhu trvání Smlouvy, i před jejím uzavřením, provést nebo nechat provést třetí stranou penetrační testování nebo testování zranitelností dodávaného řešení.

b) Dodavatel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost k provedení testů.

c) Pokud výsledky testování odhalí kritická nebo vysoce závažná zjištění, Dodavatel bez zbytečného odkladu a na vlastní náklady přijme účinná nápravná opatření k odstranění zjištěných zranitelností.

d) Plán nápravných opatření podléhá schválení Objednatele.

e) S výsledky testování se seznámí výhradně pověřené osoby Dodavatele a Objednatele.

8.4 Bezpečná konfigurace

a) Dodavatel odpovídá za bezpečnou konfiguraci všech jím dodávaných systémů v souladu s uznávanými standardy (např. CIS Benchmarks) a specifickými požadavky Objednatele, pokud byly stanoveny.

b) Dodavatel předá Objednateli dokumentaci popisující provedená konfigurační opatření a nastavení.

8.5 Řízení změn

a) O plánovaných změnách v dodávaném řešení Dodavatel s dostatečný předstihem informuje Objednatele, který zhodnotí jejich dopad a případně provede analýzu souvisejících rizik a navrhne opatření ke snížení případných nepříznivých dopadů. Významnost změny posuzuje Objednatel.

b) Dodavatel poskytne Objednateli veškerou nezbytnou součinnost při analýze rizik, aktualizaci bezpečnostní dokumentace a souvisejícím testování.

c) Pro každou významnou změnu Dodavatel zajistí možnost návratu do původního stavu (rollback).

9. Ochrana dat a informací

9.1 Nakládání s daty Objednatele

a) Dodavatel užívá Data Objednatele výhradně za účelem řádného plnění předmětu Smlouvy a pouze v nezbytném rozsahu.

b) Jakékoli jiné použití, kopírování, modifikace nebo zpřístupnění třetím stranám se bez předchozího písemného souhlasu Objednatele přísně zakazuje.

c) Dodavatel se zavazuje nakládat s daty v souladu se Smlouvou a příslušnými právními předpisy.

9.2 Kryptografická ochrana

a) Dodavatel uchovává a přenáší veškeré Důvěrné informace (např. identifikační údaje certifikátů, hesla, přístupová oprávnění, konfigurační soubory) poskytnuté Objednatelem nebo generované v rámci plnění výhradně v šifrované podobě a chrání je proti neoprávněnému přístupu.

b) Použité kryptografické algoritmy a délky klíčů musí odpovídat aktuálně platným doporučením Národního úřadu pro informací a kybernetickou bezpečnost. Ta Dodavateli mohou být předána na vyžádání.

9.3 Bezpečnost síťové komunikace

a) Dodavatel zabezpečuje veškerý přenos Dat Objednatele prostřednictvím veřejných i soukromých sítí pomocí silných a aktuálně odolných kryptografických protokolů.

b) Dodavatel chrání on-line transakce realizované prostřednictvím webových technologií platnými certifikáty SSL/TLS vydanými důvěryhodnou certifikační autoritou.

c) Dodavatel chrání všechny informační systémy Dodavatele, které se připojují do síťové infrastruktury Objednatele, aktuálním a řádně konfigurovaným řešením detekujícím a odstraňujícím škodlivý kód.

9.4 Likvidace dat a nosičů

a) Pokud má Dodavatel v rámci plnění Smlouvy povinnost provést mazání Dat Objednatele nebo likvidaci technických nosičů, postupuje vždy v souladu s uznávanými standardy pro bezpečnou likvidaci dat.

b) Pokud není klasifikace informace určena, použije se způsob likvidace stanovený pro nejvyšší úroveň důležitosti aktiva.

c) Přípustné způsoby likvidace zahrnují bezpečné přepsání, degaussing nebo fyzickou likvidaci nosiče informace.

d) Dodavatel o provedené likvidaci vyhotoví protokol a předá jej Objednateli.

10. Monitorování a zvládání kybernetických bezpečnostních incidentů

10.1 Zaznamenávání činností

a) Předmět plnění, má-li podobu softwarového nebo kombinovaného řešení, musí poskytovat auditní záznamy (logy) o činnostech v něm provedených, a to v rozsahu, který umožní jednoznačně určit uživatele, čas a provedenou činnost.

b) Dodavatel se zavazuje umožnit přístup k auditním záznamům Objednateli v takové podobě, aby je bylo možné centralizovaně zpracovávat nástrojem pro správu bezpečnostních informací a událostí (SIEM)

10.2 Detekce a hlášení kybernetických bezpečnostních událostí a incidentů

a) Dodavatel neprodleně, nejpozději však do tří (3) hodin po jejich zjištění, informuje Objednatele o všech kybernetických bezpečnostních událostech či incidentech souvisejících s plněním předmětu Smlouvy.

b) Dodavatel provádí hlášení telefonicky na kontaktní linku Objednatele, kterou je Bezpečnostní dispečink (+420 602 238 151) a zároveň písemně na emailovou adresu (bd@airport-ostrava.cz).

c) Oznámení musí obsahovat popis povahy případu, dotčených aktiv, předpokládaného dopadu a sdělení, jaká opatření již Dodavatel ve vztahu k danému incidentu či události provedl.

10.3 Součinnost při řešení incidentů

a) Při vyhodnocování příčin a dopadů kybernetického bezpečnostního incidentu, který souvisí s předmětem Smlouvy, poskytne Dodavatel Objednateli plnou a bezodkladnou součinnost.

b) Součinnost zahrnuje zejména poskytnutí logů, identifikačních údajů (např. IP adresa, MAC adresa), poskytnutí obrazů paměti nebo disků pro forenzní analýzu a realizaci nápravných a mitigačních opatření požadovaných Objednatelem.

c) V případě, že Dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel, provede na své náklady analýzu kořenových příčin (Root Cause Analysis) a navrhne Objednateli ke schválení soubor technických a organizačních opatření s cílem zamezit opakování incidentu.

d) Objednatel se v případě, že nastane závažný kybernetický incident, může se obrátit na NÚKIB, pokud dodavatel odmítne nebo nereaguje na výzvy objednatele na žádost o data. Dodavatel musí data předat ihned (zároveň má Dodavatel nárok na úhradu nákladů po předání dat – tzv. účelné náklady).

11. Řízení kontinuity činností

a) Objednatel může zapojit Dodavatele do svého systému řízení kontinuity činností. To zahrnuje zejména oprávnění zahrnout Dodavatele a jím poskytované služby do plánů kontinuity činností a havarijních plánů Objednatele.

b) Dodavatel se zavazuje poskytnout nezbytnou součinnost při pravidelných odstávkách, v případě mimořádné události nebo při testování plánů kontinuity a obnovy Objednatele.

12. Požadavky na systémovou a provozní dokumentaci

a) Nejpozději do doby předání a převzetí plnění Dodavatel dodá kompletní systémovou a provozní bezpečnostní dokumentaci. Nedodání dokumentace se považuje za významnou vadu bránící převzetí plnění.

b) Systémová dokumentace musí obsahovat popis funkcí a činností nezbytných pro správu a užívání dodaného řešení, včetně uživatelské a administrátorské příručky.

c) Provozní bezpečnostní dokumentace musí obsahovat popis nezbytných bezpečnostních funkcí (např. způsob aktualizace, možnosti logování, postupy pro zálohování a obnovu, instalační a konfigurační postupy).

13. Řízení dodavatelského řetězce

13.1 Schvalování a řízení poddodavatelů

a) Dodavatel nezapojí do poskytování plnění dle Smlouvy žádného dalšího Poddodavatele bez předchozího, konkrétního a písemného souhlasu nebo zadání Objednatele.

b) Před udělením souhlasu si Objednatel může vyžádat od Dodavatele veškeré informace potřebné k provedení vlastního posouzení rizik spojených s navrhovaným Poddodavatelem.

c) Objednatel se zavazuje, že poddodavatelé, kteří neposkytují klíčové části plnění, nebudou mít přístup k Datům Objednatele.

13.2 Přenos a vymáhání bezpečnostních povinností

a) Dodavatel smluvně zaváže každého svého Poddodavatele k dodržování všech povinností stanovených v Příloze v plném nebo redukovaném rozsahu odpovídajícímu jeho zapojení. Na základě písemné výzvy Objednatele Dodavatel předloží k prokázání splnění této povinnosti

vhodně anonymizovanou smlouvu s Poddodavatelem.

b) Dodavatel nese plnou a výlučnou odpovědnost za jakékoli jednání či opomenutí svých Poddodavatelů, jako by šlo o jeho vlastní jednání či opomenutí.

c) Jakékoli porušení Přílohy ze strany Poddodavatele se bude považovat za přímé porušení Smlouvy ze strany Dodavatele.

ČÁST III: Kontrola, sankce a ukončení

14. Kontrola

14.1 Právo Objednatele na kontrolu

a) Objednatel má právo provádět kontroly za účelem ověření, že Dodavatel plní povinnosti vyplývající z Přílohy. Počet a frekvence kontrol nejsou omezeny.

b) Objednatel oznámí Dodavateli záměr provést kontrolu písemně, a to nejméně 14 dnů předem, ledaže by závažný bezpečnostní incident nebo podezření na něj odůvodňovaly provedení kontroly bezodkladně.

14.2 Povinnost součinnosti a nápravy zjištění

a) Dodavatel poskytne Objednateli veškerou potřebnou součinnost při kontrole, zejména zpřístupní veškerou relevantní dokumentaci, umožní přístup do prostor a k informačním systémům a zajistí přítomnost svých odpovědných zástupců.

b) S výsledky kontroly seznámí Objednatel Dodavatele formou kontrolní zprávy a poskytne mu přiměřenou lhůtu k vyjádření.

c) Dodavatel bez zbytečného odkladu přijme nápravná opatření k odstranění všech zjištěných nedostatků ve lhůtě dohodnuté s Objednatelem.

d) Nesplnění této povinnosti se považuje za podstatné porušení Smlouvy.

15. Povinnosti při ukončení smlouvy

15.1 Plán ukončení spolupráce

a) Dodavatel se zavazuje ve spolupráci s Objednatelem vypracovat a po dobu trvání Smlouvy průběžně aktualizovat Plán ukončení spolupráce tzv. Exit plán (dále jen „Plán“).

b) Plán detailně popíše postupy, odpovědnosti a časový harmonogram pro plynulé převedení všech činností spojených s plněním Smlouvy na Objednatele nebo na nového dodavatele.

c) Plán zahrne zejména postupy pro migraci dat, předání dokumentace, předání znalostí a bezpečnou likvidaci všech Dat Objednatele ze systémů Dodavatele.

15.2 Součinnost při přechodu

Dodavatel poskytne veškerou nezbytnou součinnost k realizaci pro realizaci hladkého ukončení spolupráce a předání činností, a to i po skončení účinnosti Smlouvy, po dobu nezbytně nutnou k zajištění kontinuity služeb.

15.3 Právo na mimořádné ukončení

Objednatel může Smlouvu jednostranně vypovědět bez výpovědní doby v případě, že dojde k významné změně kontroly nad Dodavatelem nebo jeho zásadními aktivy a uvedená změna dle odůvodněného posouzení Objednatele představuje nepřijatelné bezpečnostní riziko.

16. Závěrečná ustanovení

16.1 Platnost a vymahatelnost

a) Pokud se jakékoli ustanovení Přílohy stane neplatným či nevymahatelným, neovlivní to platnost a vymahatelnost ostatních ustanovení.

b) Smluvní strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož smysl a účel se co nejvíce přiblíží původnímu záměru.

c) Dodavateli nenáleží za plnění povinností dle Přílohy žádná další odměna nad rámec ceny sjednané ve Smlouvě, neboť náklady na zajištění bezpečnosti jsou nedílnou součástí řádného plnění.

16.2 Změny a dodatky

Smluvní strany mohou Přílohu měnit a doplňovat pouze prostřednictvím písemných, vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran.