

## Zajištění opatření v oblasti informační a kybernetické bezpečnosti

„Smluvní zajištění opatření v oblasti informační a kybernetické bezpečnosti ve smyslu § 8, odst. 2 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů“

### 1. Preambule

- 1.1 Dodavatel bere na vědomí, že je významným dodavatelem dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti pro objednatele Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s. p.), který je správcem informačních a komunikačních systémů kritické informační infrastruktury.
- 1.2 Informačním/komunikačním systémem, k němuž se vztahuje role významného dodavatele, je: **AGVN, AGVN2.**
- 1.3 Dodavatel se zavazuje dodržovat požadavky systému řízení bezpečnosti chráněných informací uvedené v této příloze smlouvy a bezpečnostních pravidlech distribuovaných v souladu s čl. 4 této přílohy smlouvy.

### 2. Definice pojmů

- 2.1 „Aktivem“ se rozumí souhrn informací a služeb, které jsou nezbytné pro provozování informačních/komunikačních systémů uvedených v čl. 1.2 této přílohy smlouvy.
- 2.2 „Bezpečnostním incidentem“ se rozumí narušení bezpečnosti chráněných informací v informačních/komunikačních systémech uvedených v čl. 1.2 této přílohy smlouvy.
- 2.3 „Bezpečnostním opatřením“ je úkon, jehož cílem je zajištění bezpečnosti chráněných informací v informačních/komunikačních systémech uvedených v čl. 1.2 této přílohy smlouvy, jeho dostupnosti a spolehlivosti v kybernetickém prostoru.
- 2.4 „Bezpečnostní politikou“ je soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.
- 2.5 „Bezpečnostní událostí“ taková událost, která může způsobit narušení bezpečnosti chráněných informací v informačních/komunikačních systémech uvedených v čl. 1.2 této přílohy smlouvy.
- 2.6 „Dodavatelem“ dodavatel dle smlouvy, který je zároveň významný dodavatel dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti.
- 2.7 „Kritickou informační infrastrukturou“ prvek nebo systém prvků nezbytný pro provozování informačních/komunikačních systémů uvedených v čl. 1.2 této přílohy smlouvy.

### 3. Bezpečnost chráněných informací

- 3.1 Dodavatel je povinen zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti informačních/komunikačních systémů uvedených v čl. 1.2 této přílohy smlouvy a vést o nich bezpečnostní dokumentaci.
- 3.2 Výchoziskem pro nastavení bezpečnostních opatření jsou požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, vyhlášky o kybernetické bezpečnosti, případně norem ČSN ISO/IEC 27001.
- 3.3 Provádění bezpečnostních opatření u dodavatele ověřuje objednatel postupem dle čl. 8 této přílohy smlouvy nebo platným certifikátem ISO/IEC 27001, případně jiným zavedeným a platným mezinárodně uznávaným systémem řízení bezpečnosti informací u dodavatele.

#### 4. Dodržování bezpečnostní politiky objednatele

- 4.1 Dodavatel je povinen dodržovat Bezpečnostní pravidla pro významné dodavatele objednatele, která jsou uvedena na následující webové stránce:

[https://www.rlp.cz/content/documents/Bezpecnostni\\_pravidla\\_pro\\_vyznamne\\_dodavatele.pdf](https://www.rlp.cz/content/documents/Bezpecnostni_pravidla_pro_vyznamne_dodavatele.pdf)

(dále jen „**bezpečnostní pravidla**“). Dodavatel tímto potvrzuje, že se s bezpečnostními pravidly seznámil a souhlasí s nimi.

- 4.2 Objednatel prostřednictvím manažera kybernetické bezpečnosti do 10ti dnů od účinnosti této smlouvy oznámí dodavateli detaily bezpečnostních standardů objednatele, a to prostřednictvím elektronicky podepsaného emailu.
- 4.3 Objednatel může bezpečnostní pravidla po uzavření smlouvy měnit, a to v souvislosti se změnami právních předpisů, rozhodnutími nebo varováními Národního úřadu pro kybernetickou a informační bezpečnost, rozhodnutími dalších správních úřadů nebo plněním nápravných opatření vyplývajících ze státního dozoru. Změny bezpečnostních pravidel budou distribuovány elektronickou (digitální) formou, a to e-mailovou zprávou, kde přílohy musí být převedeny do formátu pdf a podepsány manažerem kybernetické bezpečnosti minimálně uznávaným elektronickým podpisem (v souladu s eIDAS) či datovou schránkou nebo písemnou (listinnou) formou s podpisem manažera kybernetické bezpečnosti, a to prostřednictvím držitele poštovní licence s potvrzením o doručení na adresu manažera kybernetické bezpečnosti dodavatele. V případě, že dodavatel do 10ti pracovních dnů od doručení oznámení o změně nevyjádří s provedenou změnou nesouhlas, platí, že se změnou souhlasí a je povinen dodržovat takto upravená bezpečnostní pravidla.
- 4.4 Dodavatel zajistí u všech svých pracovníků, kteří se podílejí na plnění povinností dle této přílohy smlouvy prokazatelné seznámení s bezpečnostními pravidly.

#### 5. Řízení změn

- 5.1 Dodavatel je povinen řídit rizika související s plněním dle smlouvy. Na vyžádání manažera kybernetické bezpečnosti objednatele nebo osob provádějících kontrolní činnost dle čl. 8 této přílohy smlouvy je povinen způsob řízení těchto rizik doložit.
- 5.2 Dodavatel bere na vědomí, že objednatel při provádění změn postupuje v souladu s § 11 vyhlášky o kybernetické bezpečnosti.
- 5.3 U významných změn provádí objednatel analýzu rizik v souladu s metodikou CRAMM, nástrojem RAMSES.
- 5.4 Dodavatel poskytne objednateli nezbytnou součinnost a bude nápomocen při řízení změn, zejména při pravidelném hodnocení rizik a kontrole zavedených bezpečnostních opatření prováděných osobami určenými objednatel. Takovou součinnost je dodavatel povinen zajistit i u svých poddodavatelů.
- 5.5 Dodavatel, který v rámci svého řešení nezbytného pro poskytování služeb dle smlouvy využije technické nebo programové prostředky společností Huawei Technologies Co., Ltd. nebo ZTE Corporation, včetně jejich dceřiných společností, v průběhu zadávacího řízení objednateli předložil analýzu rizik zpracovanou v souladu s metodikou Národního úřadu pro kybernetickou bezpečnost.

#### 6. Informační povinnost

- 6.1 Dodavatel bezodkladně informuje objednatele prostřednictvím manažera kybernetické bezpečnosti, pokud zjistí narušení bezpečnosti chráněných informací v důsledku kybernetické bezpečnostní události a poskytne objednateli dostatečné informace, které umožní odstranit následky takové události, vyšetřit ji a ohlásit ji Národnímu úřadu pro kybernetickou bezpečnost

v souladu s požadavky vyhlášky o kybernetické bezpečnosti. Dodavatel je povinen při těchto úkonech spolupracovat a přijmout finančně přiměřené kroky, které si objednatel vyžádá.

- 6.2 Dodavatel prostřednictvím manažera kybernetické bezpečnosti průběžně a bezodkladně informuje objednatele o všech jemu známých významných a kritických hrozbách a zranitelnostech, které by mohly mít vliv na hodnocení rizik prováděných objednatelem.
- 6.3 Dodavatel prostřednictvím manažera kybernetické bezpečnosti objednatele bezodkladně informuje objednatele o významné změně ovládnutí dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných dodavatelem k plnění podle smlouvy s objednatelem. Má se za to, že významnou změnou ovládnutí se rozumí změna ovládající osoby dle § 74 a násl. zákona č. 90/2012, Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů.
- 6.4 Podrobnější podmínky ohlašování a klasifikace událostí jsou uvedeny v bezpečnostních pravidlech.

## 7. Poddodavatelé

- 7.1 Dodavatel objednatele dle § 105 odst. 4 ve spojení s odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, předem písemně informuje o úmyslu využít poddodavatele, kterého neoznámil v průběhu zadávacího řízení, včetně jeho identifikace a detailů činností, které má poddodavatel provádět a zpřístupňovaných dat. Identifikační údaje poddodavatelů, kteří se po uzavření smlouvy zapojí do plnění veřejné zakázky, předmět činností, které má poddodavatel provádět a zpřístupňovaná data, je dodavatel povinen objednateli sdělit před zahájením plnění ze strany dotyčného poddodavatele.
- 7.2 Pokud dodavatel sjedná s poddodavatelem provádění činností nebo zpřístupňování dat ve smyslu této přílohy smlouvy, je povinen uzavřít s poddodavatelem smlouvu nebo jiný právní akt, jež zakládá stejná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti jako jsou stanovené v této příloze smlouvy. Jedná se zejména o poskytnutí dostatečných záruk pro provedení vhodných technických a organizačních opatření tak, aby zpracování odpovídalo požadavkům vyhlášky o kybernetické bezpečnosti.
- 7.3 Ve vztahu ke každému poddodavateli, dodavatel:
  - a) vynaloží veškeré přiměřené úsilí, aby prověřil, že poddodavatel poskytuje úroveň ochrany v oblasti informační a kybernetické bezpečnosti, jež je vyžadována smlouvou;
  - b) zajistí, aby při řetězení poddodavatelů byla vzájemná práva a povinnosti ve vztahu k informační a kybernetické bezpečnosti upravena písemnou smlouvou obsahující podmínky, které nabízejí alespoň stejnou úroveň ochrany jako ty, které jsou uvedeny ve smlouvě a splňují požadavky příslušných právních předpisů vztahujících se ke smluvnímu plnění;
  - c) poskytne na vyžádání objednateli kopie vybraných částí smluv s poddodavateli (nebo obdobné podklady) relevantních pro plnění smlouvy;
  - d) zajistí v rozsahu jeho činnosti, aby každý poddodavatel plnil povinnosti vyplývající z smlouvy, které se vztahují na ochranu v oblasti informační a kybernetické bezpečnosti prováděnou tímto poddodavatelem, jako by byl stranou této smlouvy namísto dodavatele.
- 7.4 V případě, že součástí uzavírané dohody s poddodavateli či mezi poddodavateli je poskytnutí bezpečnostních pravidel, je dodavatel povinen o této skutečnosti informovat objednatele předem. Objednatel je oprávněn do pěti pracovních dnů od doručení oznámení o nutnosti poskytnutí bezpečnostních pravidel poddodavatelům namítnout, že poskytnutí bezpečnostních pravidel poddodavatelům není nezbytně nutné nebo že poskytnutí bezpečnostních pravidel konkrétnímu poddodavateli znamená pro objednatele bezpečnostní riziko a následně dodavateli poskytnutí

těchto bezpečnostních pravidel poddodavatelům nebo konkrétnímu poddodavateli zakázat. V takovém případě musí dodavatel prokázat nezbytnou potřebu poskytnutí těchto bezpečnostních pravidel konkrétnímu poddodavateli nebo navrhnout využití jiného poddodavatele. Jestliže objednatel tuto potřebu shledá důvodnou nebo nevyhodnotí nového poddodavatele jako bezpečnostní riziko, povolí poskytnutí těchto bezpečnostních informací konkrétnímu poddodavateli.

## 8. Kontrola

- 8.1 Dodavatel zpřístupní na vyžádání všechny informace nezbytné pro prokázání souladu s touto přílohou smlouvy a umožní a bude nápomocen při auditech a inspekcích prováděných jakýmkoli auditorem pověřeným objednatelem. Takovou součinnost je dodavatel povinen zajistit i u svých poddodavatelů.
- 8.2 S přiměřeným předstihem před zahájením kontroly informuje objednatel dodavatele o této kontrole. Objednatel dále vynaloží přiměřené úsilí, aby prováděním kontroly nedošlo ke vzniku škody, nadměrnému narušení prostor, zařízení, personálu a činnosti dodavatele. Dodavatel není povinen při provádění kontroly umožnit přístup do svých prostor pouze v případě, že:
  - a) osoba provádějící kontrolu nepředloží doklad totožnosti a pověření k provedení kontroly;
  - b) je kontrola prováděna mimo běžnou pracovní dobu, ledaže kontrola pro splnění svého účelu vyžaduje provedení právě mimo běžnou pracovní dobu a kontrolující předem (v běžnou pracovní dobu) oznámil dodavateli, že se jedná o takový případ.
- 8.3 Dodavatel bere na vědomí, že objednatel provádí periodické hodnocení dodavatelů v souladu s požadavky normy ČSN ISO/IEC 9001.