

2. Preambule

2.1 Dne 2.5.2018 byla mezi smluvními stranami podepsána Servisní smlouva č. 400/2017/PS/030 „Záložní zdroje UPS“, ev. č. objednatele 400/2017/PS/030, jejímž předmětem bylo poskytování servisní a technické podpory a údržby UPS v objektech objednatele, a která byla změněna dodatkem č. 1 ze dne 25. 11. 2021 (dále jen „**smlouva**“).

2.2 Vzhledem ke skutečnosti, že:

2.2.1 dne 1.11.2025 nabyl účinnosti zákon č. 264/2025 Sb., zákon o kybernetické bezpečnosti, který má vliv na práva a povinnosti smluvních stran smlouvy;

2.2.2 objednatel má zájem provést změny smlouvy související s prováděním plateb objednatele dle smlouvy;

se smluvní strany dohodly na této změně smlouvy, která není podstatnou změnou smlouvy podle § 222 odst. 3 zákona č. 134/2016 Sb., zákona o zadávání veřejných zakázek:

3. Předmět dodatku

3.1 Do smlouvy se doplňují nové články 5.5, 5.6 a 5.7, které zní takto:

„5.5 Veškeré platby objednatele za plnění dle této smlouvy budou prováděny na účet poskytovatele uvedený v čl. 1 smlouvy. Toto číslo bankovního účtu musí být uvedeno na každé faktuře vystavené poskytovatelem, jinak bude faktura vrácena poskytovateli k opravě. Případná změna účtu poskytovatele musí být provedena dodatkem k této smlouvě.

5.6 Pokud je poskytovatel plátcem DPH v ČR, musí být ke dni splatnosti faktury bankovní účet poskytovatele uvedený v čl. 1 smlouvy zveřejněn v registru plátců DPH vedeném MF ČR. V opačném případě není objednatel povinen příslušnou platbu provést a je oprávněn poskytovateli vrátit fakturu zpět k opravě.

*5.7 Poskytovatel je oprávněn postoupit a/nebo zastavit své pohledávky vůči objednateli pouze po předchozím písemném souhlasu objednatele uděleném prostřednictvím komunikace uskutečněné (i) elektronickými (digitálními) prostředky (např. e-mailovou zprávou), kde předmět komunikace musí být uveden v příloze převedené do formátu pdf a podepsané uznávaným elektronickým podpisem vydaným podle zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, nebo (ii) prostřednictvím datové schránky nebo (iii) poštou prostřednictvím držitele poštovní licence s potvrzením o doručení (dále jen „**ověřená komunikace**“).“*

3.2 Článek 8.5 smlouvy se zrušuje.

3.3 Článek 9.4 smlouvy se mění a nově zní takto:

„9.4 Vzhledem k tomu, že poskytovatel byl vyhodnocen jako významný dodavatel ve smyslu příslušných právních předpisů, smluvní strany se dohodly, že nedílnou součástí smlouvy je příloha č. 3. Poskytovatel je povinen plnit povinnosti stanovené touto přílohou č. 3 smlouvy. Kontaktní údaje manažerů kybernetické bezpečnosti předají druhé smluvní straně kontaktní osoby oprávněné k jednání ve věcech technických uvedené v článku 1 této smlouvy prostřednictvím ověřené komunikace. Tyto kontaktní údaje/osoby mohou být čas od času měněny, nicméně každá taková změna musí být druhé smluvní straně neprodleně oznámena prostřednictvím kontaktních osob formou ověřené komunikace. V případě rozporu mezi zněním (i) přílohy č. 3 smlouvy a (ii) smlouvy, je rozhodující znění přílohy č. 3 smlouvy.

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, se smluvní strany zavazují v dobré víře zahájit jednání, aby bez zbytečného odkladu došlo k uzavření dodatku upravujícího tuto smlouvu do podoby vyhovující těmto změnám, rozhodnutím, varováním, upozorněním či požadavkům nápravných opatření.“

3.4 Článek 11.4 smlouvy se zrušuje.

3.5 Články 11.7, 11.8, 11.9 smlouvy se mění a nově zní takto:

„11.7 Pokud poskytovatel poruší povinnosti stanovené v článku 2.4 přílohy č. 3 této smlouvy, objednatel je oprávněn požadovat zaplacení smluvní pokuty ve výši 100 000 Kč za každý jednotlivý případ porušení.

11.8 zrušen

11.9 zrušen“

3.6 Článek 13.2 smlouvy se mění tak, že se text pod písm. d) nahrazuje následovně:

„d) porušil ustanovení přílohy č. 3 této smlouvy.“

3.7 Článek 13.5 smlouvy se mění a nově zní takto:

„13.5 Objednatel je od této smlouvy dále oprávněn odstoupit v případě významné změny kontroly nad poskytovatelem nebo změně kontroly nad zásadními aktivy využívanými poskytovatelem k plnění podle této smlouvy, přičemž významnou změnou kontroly 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. Objednatel je oprávněn od této smlouvy odstoupit rovněž v případě, že objednateli vznikne povinnost ukončit tuto smlouvu z důvodů stanovených obecně závaznými právními předpisy nebo na základě pokynu Národního úřadu pro kybernetickou a informační bezpečnost.“

3.8 Příloha č. 3 smlouvy se mění a nově zní jako je uvedeno v příloze č. 1 tohoto dodatku (Bezpečnostní pravidla pro významné dodavatele).

4. Závěrečná ustanovení dodatku

4.1 Ostatní ustanovení smlouvy, která nejsou dotčena tímto dodatkem, zůstávají v platnosti beze změn.

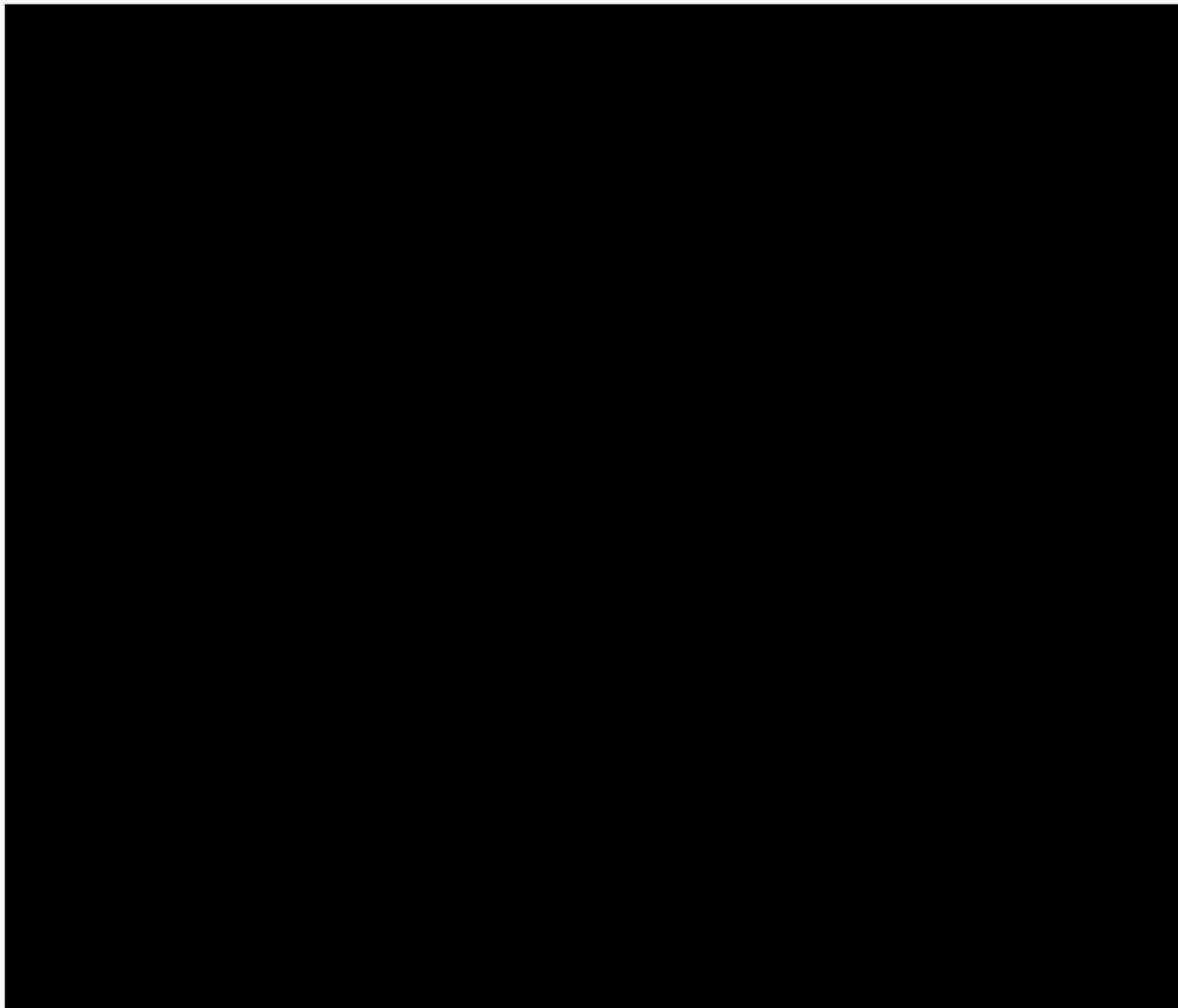
4.2 Poskytovatel bere na vědomí, že objednatel je povinen uveřejnit tento dodatek ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Poskytovatel bere rovněž na vědomí, že objednatel má povinnosti stanovené zákonem č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

4.3 Tento dodatek vstupuje v platnost dnem podpisu obou smluvních stran a účinnosti nabývá dnem jeho uveřejnění v registru smluv.

4.4 **Tento dodatek se uzavírá elektronicky, a to pouze v jednom elektronickém vyhotovení.**

4.5 Nedílnou součástí dodatku jsou tyto přílohy:

- Příloha č. 1 – nové znění přílohy č. 3 smlouvy – Bezpečnostní pravidla pro významné dodavatele



1 BEZPEČNOSTNÍ PRAVIDLA A POŽADAVKY PRO VÝZNAMNÉ DODAVATELE ŘLP ČR, S.P.

- 1.1 Bezpečnostní pravidla pro významné dodavatele stanovují základní požadavky v oblasti kybernetické bezpečnosti v souladu se zákonem č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZKB“) a vyhláškou č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „VoKB“).

2 ŘÍZENÍ INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI

- 2.1 Dodavatel má povinnost ve svých interních procesech realizovat tato opatření:
- 2.1.1 stanovit plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí v následující formě, obsahu a rozsahu:
- a) poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a poddodavatelů o jejich povinnostech a o bezpečnostní politice;
 - b) potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;
- 2.1.2 určit osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;
- 2.1.3 v souladu s plánem rozvoje bezpečnostního povědomí zajistit poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a poddodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;
- 2.1.4 pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajistit pravidelná odborná školení, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti;
- 2.1.5 v souladu s plánem rozvoje bezpečnostního povědomí zajistit pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;
- 2.1.6 zajistit kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a má nastaven proces disciplinárního řízení pro své zaměstnance;
- 2.1.7 v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajistit předání odpovědností;
- 2.1.8 hodnotit účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí;
- 2.1.9 určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;
- 2.1.10 evidovat informace o osobách, které se podílejí na plnění předmětu smlouvy, a to včetně dokumentace o absolvovaných školeních v oblasti kybernetické bezpečnosti a jejich obsahu.
- 2.2 Využívá-li dodavatel při poskytování předmětu plnění poddodavatele, je povinen zajistit adekvátní dodržování těchto bezpečnostních pravidel rovněž ve smluvních vztazích se svými poddodavateli.
- Poddodavatel je povinen plnit stejné bezpečnostní povinnosti jako dodavatel a dodržovat veškerá ujednání mezi dodavatelem a ŘLP, která se vztahují na poskytování předmětu plnění. Dodavatel nese odpovědnost za činnost poddodavatele ve stejném rozsahu, jako by plnění prováděl sám.
- 2.3 ŘLP si vyhrazuje právo 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 ŘLP nesoulad dodavateli a obě strany vejdu v jednání pro řešení této situace.

- 2.4 ŘLP je oprávněno požadovat po dodavateli smluvní pokutu, a to za každý jednotlivý případ porušení požadavků na ochranu kybernetické bezpečnosti:
- a) nezabezpečení koncové pracovní stanice dle bodu 6.6.
 - b) nedodržení zásad používání VPN dle bodu 6.6
 - c) porušení ohlašovacích povinností dle bodu 13.1
 - d) nezajištění auditních nálezů dle bodu 14.8
 - e) porušení závazků týkajících se řízení poddodavatelů dle bodu 15
- 2.5 ŘLP je oprávněno požadovat po dodavateli smluvní pokutu za každý jednotlivý případ porušení povinnosti ochrany důvěrných informací nebo povinnosti mlčenlivosti ohledně důvěrných informací.
- 2.6 Dodavatel je povinen zavést a provádět bezpečnostní opatření pro zajištění ochrany chráněných informací ŘLP. O přijatých opatřeních vede dodavatel dokumentaci a na požádání ji zpřístupní ŘLP.
- Chráněnými informacemi se rozumí veškeré údaje nebo informace, které představují hodnotu pro ŘLP a jež nejsou obecně známy konkurentům a veřejnosti. Chráněné informace lze rovněž označit jako důvěrné informace (např. v NDA).
- 2.6.1 bezpečnostní opatření musí být nastavena v souladu s požadavky ZKB a VoKB. V odůvodněných případech lze uplatnit také mezinárodní normy řady ISO/IEC 27xxx, pokud lépe odpovídají charakteru poskytovaných služeb a typu dodavatele;
- 2.6.2 dodavatel zajistí, že přístup k chráněným informacím budou mít pouze jím pověřené osoby, kterým byl zřízen privilegovaný přístup k informacím nebo aktivům ŘLP;
- 2.6.3 provádění bezpečnostních opatření u dodavatele ověřuje ŘLP formou auditu, jehož náležitosti jsou specifikovány v části Audit dodavatele tohoto dokumentu. Dodavatel může rovněž prokázat splnění požadavků předložením platného certifikátu systému řízení bezpečnosti informací dle ISO/IEC 27001, nebo jiným mezinárodně uznávaným osvědčením. Takové certifikace však žádným způsobem nenahrazují ani nenarušují práva a povinnosti vyplývající z části Audit dodavatele.

3 PERSONÁLNÍ BEZPEČNOST

- 3.1 Dodavatel zajistí seznámení všech osob, účastnících se plnění dle uzavřené smlouvy s ŘLP, s těmito bezpečnostními pravidly a dalšími upřesňujícími bezpečnostními informacemi prokazatelně předanými ze strany ŘLP. Tyto osoby stvrdí seznámení písemně.
- 3.2 Osoby, účastnící se plnění dle uzavřené smlouvy s ŘLP, musí mít prokazatelné potřebné kvalifikační předpoklady, zkušenosti a znalosti.
- 3.3 Dodavatel musí zajistit, aby osoby, účastnící se plnění dle uzavřené smlouvy s ŘLP, prošly procesem prověřování a byly jim stanoveny podmínky a odpovědnosti pro jejich činnosti.

4 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 ŘLP.

5 ŘÍZENÍ PROVOZU DODAVATELE

- 5.1 Dodavatel se zavazuje:
- 5.1.1 zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění v souladu s požadavky VoKB a doporučeními technických norem řady ISO/IEC 27xxx;

- 5.1.2 na vyžádání poskytnout ŘLP přehled o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře, kterými plní předmět smlouvy.

6 ŘÍZENÍ PŘÍSTUPU

- 6.1 Jakékoliv zásahy do systémů ŘLP je možné vykonávat:
- a) pouze po souhlasu a s koordinací odpovědného pracovníka ŘLP;
 - b) pokud možno v období minimálního provozního využití systémů, tj. typicky nočních hodin.
- 6.2 Pracovníci dodavatele musí být před zahájením prací prokazatelně proškoleni o specifických rizicích spojených s prací na jednotlivých systémech a o pravidlech pro používání VPN. Školení provede odpovědný zaměstnanec ŘLP buď přímo se všemi oprávněnými pracovníky dodavatele, nebo prostřednictvím určené osoby dodavatele, která následně zajistí proškolení celého týmu. Ve druhém případě je dodavatel povinen na vyžádání ŘLP doložit informace o proškolení svých pracovníků.
- 6.3 Identifikace
- 6.3.1 každý zaměstnanec dodavatele podílející se na plnění smlouvy s ŘLP 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. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji;
- 6.3.2 stejné pravidlo platí pro přístup k internímu informačnímu systému ŘLP, kde přiřazení specifických rolí dodavatele souvisí výhradně s plněním předmětu smlouvy.
- 6.4 Autentizace
- 6.4.1 podmínky pro autentizaci při využití ICT infrastruktury ŘLP:
- a) k jednoznačné identifikaci privilegovaných uživatelů určených systémů se využívá vícefaktorová autentizace;
 - b) ověření heslem – pokud není možné jednoznačně ověřit identitu privilegovaných uživatelů pomocí vícefaktorové autentizace, je použita autentizace pomocí kryptografických klíčů se zaručením obdobné úrovně bezpečnosti nebo hesla s definovanými pravidly.
- 6.5 Autorizace
- 6.5.1 zaměstnanci dodavatele jsou povinni v ICT infrastruktuře ŘLP 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;
- 6.5.2 zaměstnanci dodavatele jsou informováni ŘLP, které informace jsou považovány za chráněné, ke kterým chráněným informacím mají přístup a jak s nimi mohou nakládat;
- 6.5.3 jakékoliv manipulace a další operace s chráněnými informacemi ŘLP, které nebyly výslovně v instrukcích uvedeny, nemá dodavatel povoleny.
- 6.6 Vzdálený přístup (VPN)
- 6.6.1 podmínky vzdáleného přístupu k systémům stanovuje ŘLP a jiný vzdálený přístup není možný;
- 6.6.2 ke vzdálenému přístupu do sítě ŘLP jsou oprávněni pouze zaměstnanci dodavatele, kteří splňují následující podmínky:
- a) o zřízení vzdáleného přístupu pro daného zaměstnance bylo prokazatelně požádáno v souladu s postupy uvedenými v příslušné smlouvě s ŘLP;

b) zaměstnanec potvrdil převzetí autentizačního tokenu a seznámení s pravidly pro jeho využívání formou předávacího protokolu.

6.6.3 povinnosti zaměstnance dodavatele související s autentizačním tokenem:

- a) zvolit si PIN, který nebude sdílet s žádnou další osobou, nebude možné ho snadno odhadnout a bude chráněn proti prozrazení jiné osobě;
- b) neumožnit přístup k VPN připojení neoprávněným osobám, nepůjčovat svůj token jiné osobě;
- c) při autentizaci dbát zobrazených pokynů;
- d) v případě fyzického poškození tokenu, jeho ztráty, prozrazení PINu nebo při podezření na zneužití tokenu tuto skutečnost neprodleně hlásit na H24 pracoviště ŘLP tel.: 220 373 030;

6.6.4 v případě závažného či opakovaného porušení těchto pravidel bude zaměstnanci dodavatele token odebrán a dodavatel bude o této skutečnosti informován prostřednictvím ŘLP;

6.6.5 koncové zařízení využitě pro připojení do sítě ŘLP musí mít:

- a) pokročilou funkční trvalou antivirovou ochranu ve skutečném čase, s pečeti AV-TEST APPROVED (av-test.org) nebo s certifikátem VB100 (virusbulletin.com) – platí pro prostředí MS Windows a Android;
- b) funkční firewall na osobních počítačích;
- c) zapnuté automatické aktualizace systému;
- d) operační systém, který není mimo servisní podporu výrobce (pokud není smluvním ujednáním výslovně stanoveno jinak);
- e) aktualizované aplikace třetích stran při dodržení autorských práv třetích stran;
- f) zajištěno šifrování všech paměťových médií, na kterých jsou uložena chráněná data a informace ŘLP. Přístup k paměťovým médiím a k dešifrování chráněných dat a informací ŘLP musí být umožněno jen oprávněným osobám dodavatele;
- g) nainstalovaného VPN klienta, instalovaného výlučně v odpovědnosti dodavatele;
- h) druhý autentizační faktor (HW nebo SMS token) pro přístup k VPN, který bude poskytnut určeným zaměstnancem ŘLP proti podpisu předávacího protokolu;

6.6.6 zaměstnanec dodavatele je povinen před připojením do systémů sdělit příslušnému supervizorovi technického sálu minimálně následující informace:

- a) důvod požadavku na vzdálený přístup;
- b) možné dopady plánované činnosti jak na systém samotný, tak na dostupnost funkcí pro uživatele systému;
- c) předpokládaná délka činnosti (připojení);
- d) potvrdit telefonické spojení;

6.6.7 supervizor technického sálu ŘLP je oprávněn neumožnit vzdálený přístup v případě:

- a) rozporu rozsahu požadované činnosti s jeho pracovními povinnostmi nebo jeho odpovědností za systémy;
- b) složité provozní situace, pokud se nejedná o nutný zásah na systému s touto situací související;
- c) podezření, že tělesný či duševní stav externích pracovníků může negativně ovlivnit provozní bezpečnost služeb poskytovaných ŘLP, respektive takové pracovníky může vykázat z prostoru ŘLP.

7 ŘÍZENÍ ZMĚN

- 7.1 Změny na straně dodavatele musí být řízeny s ohledem na kritičnost informací, systémů a procesů souvisejících s plněním předmětu smlouvy a opětovným posuzováním rizik.
- 7.2 Dodavatel se zavazuje:
- 7.2.1 řídit rizika související s plněním předmětu dle smlouvy;
- 7.2.2 na vyžádání zástupce ŘLP doložit způsob řízení rizik;
- 7.2.3 informovat ŘLP o zbytkových rizicích a o způsobu jejich řízení;
- 7.2.4 řídit a evidovat změny v poskytovaných službách v souladu s požadavky VoKB a doporučeními technických norem řady ISO/IEC 27xxx;
- 7.2.5 poskytnout ŘLP veškeré nezbytné informace a podklady potřebné pro řízení významných změn a zajistit, aby stejnou povinnost plnili i jeho poddodavatelé. Za významnou změnu se považuje taková změna, která má nebo může mít závažný dopad na úroveň kybernetické bezpečnosti ŘLP a souvisí s předmětem plnění smlouvy.
- a) vyhodnotit každou významnou změnu;
 - b) neprodleně oznámit ŘLP plánované významné změny;
 - c) vyžádat souhlas ŘLP s provedením významné změny;
 - d) zajistit dostatečné otestování všech změn před nasazením do produkčního prostředí, pokud to charakter změny vyžaduje;
 - e) evidovat všechny změny, včetně jejich testování, schválení a dopadů;
 - f) aktualizovat příslušnou bezpečnostní dokumentaci v návaznosti na schválené a otestované změny;
- 7.3 Dodavatel odpovídá za to, že žádná změna nebude mít negativní dopad na bezpečnost poskytovaného plnění a že bude provedena v souladu s požadavky ŘLP a platnou legislativou.

8 AKVIZICE, VÝVOJ A ÚDRŽBA

- 8.1 Dodavatel se zavazuje:
- 8.1.1 zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění smlouvy s ŘLP nebo s tímto předmětem souvisí;
- 8.1.2 dodržovat úroveň poskytovaných služeb v souladu s podmínkami smlouvy, nebo SLA, pokud je taková dohoda součástí smluvního vztahu;
- 8.1.3 předat ŘLP dokumentaci předmětu plnění minimálně v následujícím rozsahu:
- a) dokumentace skutečného provedení;
 - b) dokumentace všech bezpečnostních nastavení, funkcí a mechanismů;
 - c) dokumentace obsahující popis autorizačního konceptu a oprávnění;
 - d) dokumentace obsahující zálohovací a archivační postupy;
 - e) dokumentace obsahující instalační a konfigurační postupy;
 - f) dokumentace zahrnující testy zranitelnosti a soulad s bezpečnostními požadavky ŘLP;
 - g) dokumentace pro zajištění kontinuity provozu a obnovy po havárii;
- 8.2 V případě, že předmětem plnění smlouvy je vývoj řešení, se dodavatel zavazuje:

- 8.2.1 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;
- 8.2.2 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.);
- 8.2.3 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 ŘLP;
- 8.2.4 zajistit bezpečnost testovacího prostředí u dodavatele a ochranu poskytnutých testovacích dat ŘLP;
- 8.2.5 zajistit, že v produkčním prostředí ŘLP bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění;
- 8.2.6 zajistit, že v rámci poskytovaného plnění bude dodávané řešení v souladu s doporučeními technických norem řady ISO/IEC 27xxx;
- 8.2.7 poskytnout ŘLP potřebnou součinnost v případě, že vyžaduje/realizuje provedení bezpečnostních testů souvisejících s předmětem plnění smlouvy;
- 8.2.8 předat zdrojový kód ŘLP, je-li tak stanoveno ve smlouvě, bezpečnou formou zajišťující jeho integritu, a v takovém případě:
- a) zajistit řízení verzí zdrojového kódu;
 - b) zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí;
 - c) zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí pro řízenou kompilaci těchto zdrojových kódů;
- 8.2.9 nevyvíjet, nekompilovat a nešířit v prostředí ŘLP programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

9 POŽADAVKY NA ÚDRŽBU A AKTUALIZACI SYSTÉMU – PLATÍ PRO SERVISNÍ SMLOUVY

9.1 Dodavatel se zavazuje:

- 9.1.1 při provádění aktualizací a upgradů softwaru dodržet následující pravidla:
- a) bez zbytečného odkladu informovat ŘLP o možnosti provedení aktualizace nebo upgradu softwaru, jakmile se zjistí, že je to možné. ŘLP má právo oznámit dodavateli, že podle jeho názoru je aktualizace nebo upgrade nutný či vhodný;
 - b) k možnosti provést aktualizaci nebo upgrade softwaru (jak softwaru třetích stran, tak vlastního softwaru) pouze s předchozím písemným souhlasem ŘLP;
- 9.1.2 informovat ŘLP o možnosti provedení aktualizace softwaru třetích stran v souladu s doporučeními příslušného výrobce softwaru třetích stran a nejnovějšími požadavky v oboru.

10 UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

- 10.1 Je-li v rámci předmětu plnění vyžadováno použití kryptografických prostředků, technické podmínky jsou následující:
- 10.1.1 šifrování symetrickým heslem nejméně metodou AES 256. Heslo musí být předáno jiným komunikačním kanálem;

- 10.1.2 šifrování pomocí digitálních certifikátů vydaných obecně uznávanou CA nebo CA, které explicitně důvěřují obě strany;
- 10.1.3 pokud nelze ověřit platnost certifikátu vůči Seznamu zneplatněných certifikátů (CRL), je certifikát považován za neplatný a nelze jej použít k šifrování nebo podpisu;
- 10.1.4 šifrování pomocí PGP klíčů odsouhlasených oběma stranami nebo ověřené nezávislou důvěryhodnou třetí stranou;
- 10.1.5 pro VPN přístup k systémům ŘLP se používá šifra AES256/SHA256 nebo silnější;
- 10.1.6 pro webové servery prezentující data pocházející ze systémů ŘLP mimo samotný systém používají HTTPS protokol minimálně se šifrou TLS 1.1;
- 10.1.7 pro webové servery prezentující data pocházející ze systémů pro uživatele mimo ŘLP se používá EV certifikát obecně uznávané certifikační autority;

11 MONITORING

- 11.1 Přístup zaměstnanců dodavatele k vybraným chráněným interním informacím a k informačním a komunikačním systémům ŘLP je nepřetržitě zaznamenáván, monitorován a vyhodnocován.
- 11.2 Události v systémech jsou ŘLP zaznamenávány do logů:
 - 11.2.1 úspěšné a neúspěšné přihlášení a odhlášení uživatelů;
 - 11.2.2 činnosti provedené administrátory;
 - 11.2.3 úspěšné a neúspěšné manipulace s účty, oprávněními a právy;
 - 11.2.4 neprovedení činností v důsledku nedostatku přístupových oprávnění;
 - 11.2.5 činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;
 - 11.2.6 zahájení a ukončení činností technických aktiv;
 - 11.2.7 automatická varovná nebo chybová hlášení technických aktiv;
 - 11.2.8 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.
- 11.3 Ke každému záznamu v logu přiřazuje ŘLP:
 - 11.3.1 datum a čas;
 - 11.3.2 typ činnosti;
 - 11.3.3 název relevantního technického aktiva;
 - 11.3.4 identifikaci uživatele;
 - 11.3.5 identifikaci síťového zařízení původce;
 - 11.3.6 úspěšnost nebo neúspěšnost provedení činnosti;
 - 11.3.7 úroveň závažnosti.
- 11.4 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.

12 OCHRANA DATOVÝCH ÚLOŽIŠŤ A PŘENOSNÝCH MÉDIÍ

- 12.1 Uložení chráněných informací ŘLP do datových úložišť, na přenosná média a případný transport médií mimo prostory ŘLP podléhá schválení manažerem kybernetické bezpečnosti ŘLP.
- 12.2 V případě ukládání chráněných informací ŘLP do datových úložišť a na přenosná média má dodavatel povinnost ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a vést evidenci těchto médií.
- 12.3 Dodavatel je povinen zajistit likvidaci operativních dat ŘLP ihned po pominutí účelu jejich zpracování nebo uložení způsobem dle standardu NIST SP 800-88. Po likvidaci dat na elektronickém médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí dodavatel vést protokol.

13 KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI/INCIDENTY

- 13.1 Dodavatel má za povinnost:
- 13.1.1 bezodkladně informovat ŘLP prostřednictvím manažera kybernetické bezpečnosti o všech jemu známých významných a kritických hrozbách a zranitelnostech, které by mohly mít vliv na hodnocení rizik prováděných ŘLP;
- 13.1.2 detekovat, sbírat a vyhodnocovat kybernetické události ohrožující bezpečnost chráněných aktiv;
- 13.1.3 bezprostředně po zjištění, nejpozději však do dvou hodin, prokazatelně nahlásit narušení bezpečnosti chráněných aktiv v důsledku kybernetického bezpečnostního incidentu na H24 pracoviště ŘLP tel.: 220 373 030 s popisem:
- a) data a času zjištění;
 - b) povahy události;
 - c) zdroje události;
 - d) cíle/oběti události;
 - e) potenciálního dopadu.
- 13.1.4 spolupracovat s ŘLP a přijmout přiměřené kroky vyžádané ŘLP při řešení kybernetického bezpečnostního incidentu.
- 13.2 V souvislosti s bezpečnostními událostmi a incidenty má navíc dodavatel následující povinnosti:
- 13.2.1 zavést bezpečnostní opatření podle požadavků ŘLP, v návaznosti na jeho vnitřní bezpečnostní politiky a metodiky např. pro hodnocení rizik, plány kontinuity nebo prohlášení o aplikovatelnosti;
- 13.2.2 přijmout a realizovat opatření na ochranu systémů a sítí před hrozbami nebo incidenty a zajistit řešení již vzniklých incidentů;
- 13.2.3 předat ŘLP data, provozní údaje a informace, které má k dispozici v souvislosti s podporovaným systémem ŘLP, a to bez zbytečného odkladu a ve sjednaném formátu;
- 13.2.4 na základě rozhodnutí NÚKIB předávat ŘLP potřebná data a informace, pokud hrozí kybernetický incident a dosud tak neučinil.

14 AUDIT DODAVATELE (ZÁKAZNICKÝ AUDIT)

- 14.1 Dodavatel je povinen umožnit ŘLP a ÚCL provést auditní přezkoumání činností a procesů, za účelem ověření souladu bezpečnostních opatření s právními předpisy, vnitřními předpisy a smluvními závazky vztahujícími se k předmětu dodávky.
- 14.2 Dodavatel je povinen poskytnout auditorovi nezbytnou spolupráci, dokumentaci, záznamy a přístup do prostor nezbytných pro realizaci předmětu smlouvy. Stejnou součinnost je dodavatel povinen zajistit i u svých poddodavatelů.

- 14.3 ŘLP oznámí dodavateli záměr provést audit s dostatečným předstihem, alespoň 30 dní předem. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že ŘLP se zavazuje vynaložit přiměřené úsilí, aby prováděním auditu nedošlo k nepřiměřenému narušení činností dodavatele.
- 14.4 Dodavatel bere na vědomí, že ŘLP provádí periodická hodnocení dodavatele v souladu s požadavky normy ČSN ISO/IEC 9001, která mimo jiné zohledňují známá rizika a provádění bezpečnostních opatření ze strany dodavatele.
- 14.5 ŘLP si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování dodavatele, závažný bezpečnostní incident) v souvislosti s plněním smlouvy provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.
- 14.6 Dodavatel není povinen při provádění auditu umožnit přístup do svých prostor pouze v případě, že:
- osoba provádějící audit nepředloží doklad totožnosti a pověření k provedení auditu nebo
 - audit je prováděn mimo běžnou pracovní dobu s výjimkou případů, že audit pro splnění svého účelu vyžaduje provedení právě mimo běžnou pracovní dobu a ŘLP o takovém případě dodavatele předem (v řádné pracovní době) informoval.
- 14.7 Dodavatel má právo vyjádřit se k závěrečné zprávě, obsahující výsledky auditu včetně shledaných auditních zjištění nebo neshod, kterou obdrží od ŘLP ve lhůtě 30 dnů od ukončení auditu. Jeho připomínky budou zohledněny při schvalování obsahu a lhůt pro nápravná opatření.
- 14.8 Dodavatel je povinen ve lhůtě 30 dní od obdržení závěrečné zprávy sdělit ŘLP, jaká nápravná opatření navrhuje k odstranění zjištěných nedostatků a kdy je provede. ŘLP tato opatření buď schválí, nebo je vrátí dodavateli s připomínkami k přepracování.
- 14.9 Dodavatel má za povinnost:
- v určeném čase zajistit realizaci dohodnutých nápravných opatření;
 - zprávu o realizovaných opatřeních oznámit a předat ŘLP neprodleně po provedení dotčených opatření;

15 PODDODAVATELÉ

- 15.1 Dodavatel je povinen předem, tj. před zahájením plnění ze strany dotyčného poddodavatele, písemně informovat ŘLP o úmyslu využít poddodavatele, kterého neoznámil v průběhu zadávacího řízení, včetně jeho identifikace a detailů činností, které má poddodavatel provádět, a zpřístupňovaných dat.
- 15.2 Pokud dodavatel sjedná s poddodavatelem provádění činností nebo zpřístupňování dat, 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 tomto dokumentu a smlouvě uzavřené mezi ŘLP a dodavatelem. Jedná se zejména o poskytnutí dostatečných záruk pro provedení vhodných technických a organizačních opatření tak, aby zpracování odpovídalo požadavkům VoKB.
- 15.3 Dodavatel ve vztahu ke každému poddodavateli:
- vynaloží veškeré přiměřené úsilí, aby prověřil, že poddodavatel poskytuje úroveň ochrany v oblasti informační a kybernetické bezpečnosti, jež je vyžadována dle této přílohy smlouvy;
 - 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 v tomto dokumentu a splňují požadavky příslušných právních předpisů vztahujících se ke smluvnímu plnění;
 - poskytne na vyžádání ŘLP 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 tohoto dokumentu a smlouvy, které se vztahují k ochraně v oblasti informační a kybernetické bezpečnosti prováděné tímto poddodavatelem, jako by byl stranou smlouvy namísto dodavatele.

15.4 Dodavatel je povinen informovat ŘLP a prokázat, že součástí uzavírané smlouvy s poddodavatelem bude poskytnutí těchto bezpečnostních pravidel poddodavateli.

16 INFORMAČNÍ POVINNOST

16.1 Dodavatel prostřednictvím manažera kybernetické bezpečnosti bezodkladně informuje ŘLP o významné změně ovládnání dodavatele podle zákona č. 90/2012, Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů nebo o změně vlastnictví zásadních aktiv, popřípadě o změně oprávnění nakládat s těmito aktivy, využívaných dodavatelem k plnění podle smlouvy s ŘLP. Má se za to, že významnou změnou ovládnání se rozumí změna ovládající osoby dle § 74 a násl. zákona o obchodních korporacích.

16.2 Dodavatel bezodkladně informuje ŘLP o každé žádosti cizozemského orgánu o zpřístupnění nebo předání dat a dále je dodavatel povinen:

- a) zpřístupnit nebo předat data pouze po důkladném přezkoumání zákonnosti žádosti, včetně souladu s právním řádem České republiky a relevantními mezinárodními předpisy;
- b) vynaložit veškeré úsilí k zabránění zpřístupnění nebo předání dat, pokud to právní řád umožňuje, a to zejména v případech, kdy by mohlo dojít k ohrožení bezpečnosti, důvěrnosti nebo integrity dat;
- c) zpřístupnit nebo předat data pouze v nezbytném rozsahu odpovídajícím konkrétní žádosti.

16.3 Pokud dodavatel v rámci svého řešení při plnění předmětu smlouvy:

- a) využije technické nebo programové prostředky, produkty nebo služby společností Huawei Technologies Co., Ltd. nebo ZTE Corporation, včetně jejich dceřiných společností, nebo
- b) bude zpracovávat systémová či uživatelská data na území Čínské lidové republiky nebo zvláštních administrativních oblastí, nebo
- c) bude vykonávat vzdálenou správu technických aktiv z území Čínské lidové republiky, zvláštních administrativních oblastí, nebo prostřednictvím subjektů usídlených na těchto územích,

je povinen v průběhu zadávacího řízení ŘLP předložit analýzu rizik zpracovanou v souladu s metodikou Národního úřadu pro kybernetickou bezpečnost (NÚKIB), která prokazatelně vyhodnotí bezpečnostní rizika spojená s využitím těchto technologií. Analýza se bude vztahovat pouze na rizika relevantní pro daný případ.

17 OCHRANA AKTIV PROTI NEAUTORIZOVANÝM ČINNOSTEM

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

Za aktivum se pro účely tohoto dokumentu považuje jakýkoli prvek informačního systému, zařízení, software, data nebo jiný prostředek, který má hodnotu pro ŘLP a je využíván při poskytování služeb nebo plnění dodávky dle této smlouvy.

18 PODMÍNKY PŘI UKONČENÍ SMLOUVY

18.1 Nejpozději k termínu ukončení smluvního vztahu ŘLP ukončí veškeré přístupy dodavatele a jeho zaměstnanců k aktivům ŘLP.

18.2 Zaměstnanci dodavatele jsou povinni vrátit poskytnutá aktiva ŘLP nejpozději k termínu ukončení smluvního vztahu.

- 18.3 Pokud byla dodavateli poskytnuta informační aktiva (data) ŘLP, musí být nejpozději k termínu ukončení smluvního vztahu vrácena a zcela smazána způsobem dle standardu NIST SP 800-88 ze všech informačních systémů dodavatele a nosičů dodavatele taková aktiva obsahujících.