Korporátní pravidla informační bezpečnosti a ochrany dat

1. Tato Korporátní pravidla informační bezpečnosti a ochrany dát (dále jen "**Pravidla**") se aplikují na závazkové vztahy mezi společností T-Mobile Czech, a.s. (dále jen "**TMCZ**" nebo „**Kupující**") a druhou smluvní stranou (dále jen "**Dodavatel**"), vznikající při jejich podnikatelské činnosti, zahrnující především nákupní objednávky vystavené TMCZ, kupní smlouvy, smlouvy o dílo a ostatní smlouvy podle zákona č. 89/2012 Sb. občanský zákoník, ve znění pozdějších předpisů i jakékoliv jiné smlouvy uzavřené mezi TMCZ a Dodavatelem (dále jen "**Smlouva**"), u kterých je předmětem především dodání movitých věcí (zboží), poskytnutí práv k software, zhotovení díla a/nebo poskytování služeb (dále jen "**Činnosti**") ze strany Dodavatele pro TMCZ (dále jen "**Plnění**").

2. Dodavatel je povinen při poskytování plnění podle Smlouvy dodržovat požadavky následujících mezinárodních standardů, jak vyplývá z následující tabulky:

Zaveden	Certifikován	Systém
Ano	Ano	Systém managementu kvality podle ISO 9001
Ano	Ano	Systém environmentálního managementu podle ISO 14001
Ano	Ano	Systém managementu bezpečnosti informací podle ISO 27001
Ano	Ano	Systém řízení kontinuity podnikání podle ISO 22301
Ano	Ano	Systém řízení služeb informačních technologií podle ISO 20000-1
Ano	Ano	Systém řízení energetického managementu podle ISO 50001

3. Dodavatel je povinen poskytovat Plnění podle Smlouvy a zabezpečit výkon Činností, ke kterým se zavázal podle Smlouvy, primárně prostřednictvím svých kmenových zaměstnanců. V případě, že Dodavatel využije subdodavatele, musí být tento subdodavatel schválen TMCZ a musí být uveden v Příloze č. 3 těchto Pravidel a/nebo Smlouvy, pokud se Dodavatel a TMCZ nedohodli jinak. Pokud se Dodavatel a TMCZ nedohodli jinak, Dodavatel není oprávněn pověřit výkonem svých povinností podle Smlouvy žádného subdodavatele bez předchozího písemného souhlasu společnosti TMCZ.

4. Pokud TMCZ udělí Dodavateli souhlas s použitím konkrétního subdodavatele, je Dodavatel povinen uzavřít se subdodavatelem smlouvu, která zabezpečí, aby subdodavatel vykonával povinnosti podle této Smlouvy za stejných podmínek a ve stejné kvalitě, jako je dohodnuto mezi TMCZ a Dodavatelem ve Smlouvě. Dodavatel je plně odpovědný za řádné a včasné plnění těchto povinností subdodavatelem. Zejména, ale ne výlučně, se subdodavatel musí zavázat k dodržování všech požadavků a povinností Dodavatele podle těchto Pravidel. Zejména musí být se subdodavatelem písemně ujednány podmínky pro přístup, práva a povinnosti týkající se zabezpečení ochrany všech technických, obchodních nebo jiných informací (dále jen "**Důvěrné informace**") s kterými se Dodavatel obeznámil po dobu trvání Smlouvy, bez ohledu na to, zda jsou tyto Důvěrné informace označeny jako důvěrné. Povinnost zabezpečit důvěrnost informací přetrvává i po ukončení Smlouvy.

5. V případě, že má Dodavatel zavedený nebo certifikovaný systém, který je uveden v bodě 2 těchto Pravidel, pak je povinen předložit TMCZ k nahlédnutí a kontrole dokumentované informace (např. dokumenty, záznamy, logy, nahrávky) související s požadavky výše popsaných systémů, a to za účelem prokázání souladu s požadavky definovanými výše, uvedenými mezinárodními standardy , jakož i se Smlouvou. V případě, že Dodavatel poskytuje plnění podle Smlouvy za pomoci a/nebo prostřednictvím schválených subdodavatelů, kteří mají některý ze systémů zavedený či certifikovaný, zajistí Dodavatel souhlas s provedením auditů i u těchto subdodavatelů, a to za účelem prověření shody s předmětnými mezinárodními standardy.

6. V případě, že Dodavatel nemá některý systém certifikovaný ani zavedený, souhlasí s provedením auditů zaměřených na prověření shody s požadavky Smlouvy. Dodavatel je povinen poskytnout zaměstnancům TMCZ nebo pověřeným osobám při výkonu auditu nebo při analýze rizik součinnost, předložit k nahlédnutí a ke kontrole dokumentované informace (např.: dokumenty, záznamy, logy, nahrávky), umožnit přístup do prostor a systémů souvisejících s Plněním podle Smlouvy. V případě, že Dodavatel poskytuje plnění podle Smlouvy za pomoci a/nebo prostřednictvím schválených subdodavatelů, kteří nemají některý ze systémů zavedený či certifikovaný, zajistí Dodavatel souhlas s provedením auditu i u těchto subdodavatelů, a to za účelem prověření shody se Smlouvou.

7. Dodavatel a jeho subdodavatelé jsou povinni v dohodnutých termínech vykonat aktivity a/nebo zavést nápravná opatření, která byla nalezena a dohodnuta jakožto výstup z auditu Dodavatele. Stejně tak jsou povinni vykonat činnosti a zavést nápravná opatření nalezená např. při testech, cvičeních, incidentech, řízení rizik. Dodavatel poskytne TMCZ veškeré informace (např. zprávy z auditů), které se týkají schopnosti Dodavatele poskytovat plnění podle Smlouvy. Pokud zavedení nápravných opatření bude trvat déle, jak 30 dní a nebude-li v konkrétním případě dohodnuta jiná lhůta a/nebo plán pro zajištění nápravy nebude schválen Dodavatelem nebo takový plán nezajistí nápravu a taktéž Dodavatel neoznámí výhrady k navrhnutým nápravným opatřením ve stanovené lhůtě, bude takový stav automaticky považován za podstatné porušení Smlouvy, přičemž TMCZ je v takovém případě oprávněna odstoupit od Smlouvy. V případě, že požadavek na zavedení nápravného opatření vznese příslušný státní orgán ve smyslu platné právní úpravy nebo je zavedení nápravného opatření nevyhnutelného z důvodu plnění zákonných povinností TMCZ nebo řešení bezpečnostního incidentu, Dodavatel je povinný poskytnout požadovanou součinnost v lhůtě stanovené TMCZ a její včasné neposkytnutí se považuje za podstatné porušení Smlouvy s právem odstoupit od Smlouvy.

8. Dodavatel musí mít zavedený systém řízení kontinuity podnikání, aby byl schopen TMCZ poskytovat plnění podle Smlouvy v případě nestandardních a neočekávaných situacích nepřetržitě a v souladu s parametry a kvalitou dohodnutou mezi smluvními stranami. Dodavatel je povinen poskytnout TMC součinnost při přípravě a provádění plánů kontinuity činností nebo obnovy po havárii v TMCZ. Dodavatel je povinen při poskytování Plnění podle Smlouvy dodržovat požadavky na řízení kontinuity podnikání uvedené v Příloze č. 2 těchto Pravidel, za předpokladu že plnění podle Smlouvy bude vyhodnocené analýzou dopadů (BIA) jako kritické a/nebo existuje zákonný důvod pro řízení Dodavatele v oblasti řízení kontinuity podnikání (BCM).

9. Dodavatel je povinný nakládat s odpady, kterých je původce či vlastníkem, v souvislosti s plněním podle Smlouvy, v souladu s obecně závaznými právními předpisy, především upravujícími oblast odpadů.

10. Zaměstnanci, personál, pověřené osoby a subdodavatelé Dodavatele (dále jen "**Pověřené osoby**") vstupující do prostor a objektů TMCZ a vykonávající tam Činnost podle Smlouvy, jsou povinní seznámit se s dokumentací bezpečnosti a ochrany zdraví při práci, požární ochrany a požárně-technickými zařízeními umístěných v prostorách jednotlivých objektů TMCZ.

11. Dodavatel se zavazuje v souladu s platnými předpisy o ochraně před požáry:
    a) dodržovat platné a závazné předpisy o ochraně před požáry;
    b) dodržovat pravidla požární bezpečnosti stanovena v provozních předpisech objektů a prostor TMCZ;
    c) zabezpečit účast Pověřených osob na školeních o ochraně před požáry, pokud se Pověřené osoby zdržují v objektech a prostorách TMCZ.

12. Dodavatel se zavazuje při plnění Smlouvy dodržovat všechny všeobecně závazné právní předpisy jako i ostatní aplikovatelné předpisy (např. ČSN) na zabezpečení bezpečnosti a ochrany zdraví při práci.

13. Dodavatel je povinen zabezpečit, aby ním Pověřené osoby dodržovali platná režimová, technická a organizační opatření upravující řízení vstupu, pohybu osob a dopravních prostředků v prostorách a objektech TMCZ. Pro vstup osob a/nebo vjezd dopravních prostředků do prostor

a objektů TMCZ vydá TMCZ Dodavateli potřebná povolení příslušným oddělením TMCZ. Dodavatel o povolení požádá prostřednictvím kontaktní osoby podle bodů 22 a 23 těchto Pravidel.

14. Za obeznámení Pověřených osob s relevantními interními předpisy TMCZ, odevzdání Přístupových prostředků určených pro Pověřené osoby odpovídá odpovědná osoba TMCZ.

15. Dodavatel je si vědom, že ním Pověřené osoby se podřídí kontrole vykonané v souladu s interními předpisy TMCZ (např. fyzická kontrola osob a dopravních prostředků, technická kontrola zařízení) při vstupu do prostor TMCZ. Pověřené osoby, které vykonávají činnost v prostorech TMCZ, jsou povinné se před vstupem do těchto prostor identifikovat (např. zaměstnaneckým průkazem, občanským průkazem, cestovním pasem).

16. V případě, že Dodavateli budou odevzdané Přístupové prostředky do prostor či objektů TMCZ, Dodavatel je povinen dodržovat interní předpisy TMCZ týkajíce se Přístupových prostředků. Dodavatel nesmí vyhotovit duplikát nebo kopii z převzatého Přístupového prostředku.

17. Dodavatel a Pověřené osoby jsou oprávněné při Plnění podle Smlouvy se zdržovat a pohybovat se v prostorech a objektech TMCZ jen v čase potřebném pro uskutečnění dohodnutých Činností, a to jen v prostorech a objektech, které jsou pro tyto Činnosti určené.

18. Smluvní strany berou na vědomí a souhlasí s tím, že veškeré informace obsažené ve Smlouvě jakož i v navazujících smlouvách a informace vyměněné mezi smluvními stranami v souvislosti s poskytováním Plnění podle Smlouvy, budou považovány za důvěrné a chráněné v rozsahu podmínek dohodnutých ve Smlouvě a/anebo dohodě o zachování důvěrnosti informací uzavřené mezi smluvními stranami (dále jen jako „**NDA**“) a/nebo prostřednictvím jiné specifické související dohody upravující podmínky ochrany informací (např. ochrana osobních údajů, kybernetická bezpečnost, atd.) (dále jen jako „**Speciální smlouva**“). Smluvní strany berou na vědomí a souhlasí s tím, že v případě odlišných ustanovení NDA a Smlouvy, mají vždy přednost ustanovení Smlouvy a v případě odlišných ustanovení Smlouvy a Speciálních smluv, mají vždy přednost ustanovení Speciální smlouvy v otázkách ochrany informací.

19. Dodavatel se zavazuje vytvořit, používat a udržovat přiměřené technické, organizační a personální bezpečnostní opatření k zajištění důvěrnosti, dostupnosti a integrity Důvěrných informací, které mu byly nebo budou poskytnuty nebo zpřístupněny ze strany TMCZ nebo jejich smluvních partnerů. Tato opatření musí být dostatečně odolná proti náhodnému a/nebo neoprávněnému zničení, ztrátě, záměně, zpřístupnění a/nebo proti jakýmkoliv formám neoprávněného užívání Důvěrných informací. Dodavatel je povinen udržovat tato opatření funkční po celou dobu užívání Důvěrných informací.

20. Při poskytování plnění podle Smlouvy je Dodavatel odpovědný za to, že Plnění bude dodáno bez vad, s náležitou péčí a v souladu s podmínkami uvedenými ve Smlouvě a Příloze č. 1 těchto Pravidel.

21. Dodavatel prohlašuje, že plnění podle Smlouvy budou jeho jménem dodána pouze prostřednictvím zaměstnanců, kteří jsou ve vztahu k charakteru Plnění bezúhonní a splňující potřebné kvalifikační předpoklady a že je tuto skutečnost schopen na vyžádání TMCZ prokázat. Tato povinnost platí obdobně pro subdodavatele, kteří se jménem Dodavatele budou podílet na poskytování Plnění.

22. Dodavatel je povinen zajistit ochranu důvěrnosti a integrity Přístupových prostředků (přístupové ID, hesla, tokeny čipové karty, vstupní karty, klíče apod.) do elektronických systémů a prostor TMCZ (dále jen “**Přístupové prostředky**“), které jsou Dodavateli zpřístupněny na základě Smlouvy a nesmí je zpřístupnit třetím osobám. Dodavatel je povinen neprodleně oznámit TMCZ ztrátu, krádež, zneužití či zničení Přístupového prostředku v souladu s bodem 28 těchto Pravidel.

23. Dodavatel se zavazuje, že poučí Pověřené osoby, které jsou povinni zejména:

a) pro vstup a výstup do a z prostor TMCZ používat výhradně hlavní vchod; ostatní vchody a východy mohou využít jen ve výjimečných situacích (např. evakuace, přínos či odnos nadměrného nákladu);
b) tam, kde je vyžadováno, prokázat se bez vyzvání při vstupu do prostor příslušnému zaměstnanci a/nebo pověřené osobě;
c) dbát, aby údaje (pokud jsou požadovány) uvedené na Přístupovém prostředku odpovídaly skutečnosti;
d) chránit Přístupový prostředek před poškozením, zničením, ztrátou, krádeží a zneužitím jinou osobou;
e) neposkytovat Přístupový prostředek jiným osobám;
f) pokud byl přidělený, tak viditelně nosit průkaz návštěvníka po celou dobu pobytu v prostorách TMCZ;
g) bezodkladně oznámit TMCZ ztrátu, krádež, poškození, zneužití Přístupového prostředku, jakož i jakoukoliv změnu údajů obsaženou na Přístupovém prostředku;
h) na vyzvání zaměstnance TMCZ se prokázat Přístupovým prostředkem;
i) neumožnit vstup do objektu TMCZ žádné osobě;
j) po ukončení smluvní činnosti vrátit Přístupový prostředek, jakož i veškeré další věci náležející TMCZ.

24. Dodavatel a veškeré osoby podílející se na poskytování Plnění podle Smlouvy jeho jménem, jsou povinni podřídit se a respektovat zavedené bezpečnostní opatření TMCZ a bezpečnostní pokyny a nejsou oprávněni provádět žádné činnosti, které by mohly tato opatření narušit nebo poškodit.

25. Dodavatel je vždy povinen informovat TMCZ, pokud některá z Pověřených osob ukončí svůj pracovní (dodavatelský) vztah s Dodavatelem a vrátit veškeré poskytnuté Přístupové prostředky, které TMCZ této osobě poskytl. V případě ztráty Přístupových prostředků je Dodavatel povinen nahradit TMCZ vzniklou škodu.

26. Důvěrné informace s velkým objemem budou mezi Smluvními stranami předávány a vyměňovány výhradně způsobem, který zaručí důvěrnost a integritu přenášených informací (např. přenosem souborů ve stanoveném typu a formátu pomocí SFTP protokolu).

27. Smluvní strany zřídí společný bod kontaktu za účelem řešení veškerých problémů, vzájemné poskytování informací, spolupráce v oblasti bezpečnosti informací a ochrany dat a určí pro tento účel kontaktní osoby. V případě změny této osoby se Dodavatel zavazuje bezodkladně určit novou kontaktní osobu a oznámit TMCZ její kontaktní informace.

28. Dodavatel je povinen bezodkladně ohlásit TMCZ jakoukoliv nestandardní situaci, podezřelé události, bezpečnostní incidenty a ztrátu Přístupového prostředku, a to prostřednictvím následujících kontaktů: e-mail: security@t-mobile.cz, tel.: +421 800 100 166.

29. Dodavatel je povinen v rámci spolupráce s TMCZ vynaložit maximální úsilí, aby zabránil pokračování bezpečnostního incidentu, předešel dalším bezpečnostním incidentům, zajistil a obnovil všechna opatření nezbytná pro ochranu dat a informací TMCZ.

30. Pokud Plnění podle Smlouvy zahrnuje výkon Činností přímo souvisejících s tím, že: (a) Dodavatel zajišťuje funkčnost technických a softwarových prostředků tvořících informační a/nebo komunikační systém TMCZ a/nebo (b) takový vztah je relevantní pro informace a/nebo komunikační systém TMCZ a Dodavatel tím naplnil znaky definované v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti (zákon o kybernetické bezpečnosti) a ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti, jsou TMCZ a Dodavatel před zahájením těchto Činností povinni uzavřít smlouvu o úrovni služeb v oblasti kybernetické bezpečnosti.

31. Pokud se Dodavatel a TMCZ ve Smlouvě nebo v jiné osobité dohodě výslovně nedohodnou jinak, Dodavatel nebude mít v rámci poskytovaní Plnění podle Smlouvy přístup k:

    a) jakýmkoliv osobním údajům zákazníků a zaměstnanců TMCZ ve smyslu Nařízení Evropského parlamentu a Rady (EÚ) 2016/679 z ze dne 27. dubna 2016 o ochraně

fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a zákona č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů,

b) jakýmkoliv údajům, které tvoří předmět telekomunikačního tajemství ve smyslu zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

32. Dodavatel je povinen zabezpečit, aby počítačový program (zdrojový a strojový kód), který dodá TMCZ v rámci Plnění, obsahoval jen kód vyvinutý v souladu s požadavky Smlouvy, požadavky Přílohy č. 1 těchto Pravidel a v souladu s aplikovatelnými standardy podle bodu 2 těchto Pravidel. Dodavatel se zejména zavazuje, že zdrojový kód nebude obsahovat žádné zlomyslné a/nebo škodlivé prvky či bezpečnostní slabiny umožňující narušení bezpečnosti Plnění, a že nebude obsahovat žádný Malware (viz definice v bodě 33) a zároveň je Dodavatel povinen zabezpečit ochranu před Malware. Přístup ke zdrojovému kódu bude Dodavatel řídit, omezovat na nevyhnutelný okruh Pověřených osob a chránit proti neoprávněné manipulaci.

33. Malware se rozumí zejména jakýkoliv počítačový program, soubor příkazů a instrukcí použitých přímo nebo nepřímo v počítači se schopností poškodit, zasahovat, narušit a/nebo jakkoliv nepříznivě ovlivnit software, počítačové programy, datové soubory a/nebo činnost jakéhokoliv hadware, mobilních a jiných koncových zařízení a/nebo síťových funkcionalit včetně virů, červů (worms), trojských koní (trojan horse), spyware, zadních vrátek (back doors) a jiných programů, které úmyslně uskutečňují jakékoliv zbytečné, narušující a/nebo ničivé funkce v rámci informačního systému.

34. Pokud se TMCZ a Dodavatel nedohodnout jinak, Dodavatel se zavazuje zabezpečit:
    a) použití samostatně vyvinutých testovacích anonymizovaných dat pro vývojové a testovací účely,
    b) ochranu důvěrnosti, dostupnosti a integrity testovacích dat,
    c) samostatné vývojové a testovací prostředí oddělené od produkčního prostředí,
    d) bezodkladnou bezpečnou prokazatelnou likvidaci testovacích dat po skončení potřeby jejich použití,
    e) před odevzdáním Plnění podle této Smlouvy do provozu akceptační testy, jejichž součástí jsou i bezpečnostní testy.

35. V případě porušení kterékoliv povinností vyplývající z těchto Pravidel je TMCZ oprávněna požadovat od Dodavatele zaplacení smluvní pokuty ve výši 2 500 000 Kč (slovy: dva miliony pět set tisíc korun českých), a to za každý jednotlivý případ. Smluvní pokuta je splatná na základě faktury vystavené TMCZ bez zbytečného odkladu po porušení smluvních povinností, a to do 14 dnů od jejího vystavení. Dodavatel se zavazuje, že smluvní pokutu zaplatí řádně a včas. Uhrazením smluvní pokuty není dotčen nárok na náhradu újmy ve výši přesahující smluvní pokutu..

PŘÍLOHA Č. 1 - PŘÍLOHA O BEZPEČNOSTI INFORMACÍ

VŠEOBECNÉ ZÁSADY

Tato Příloha o bezpečnosti informací (Information Security Annex, dále jen „**ISA**“) stanoví opatření v oblasti bezpečnosti informací ve společnosti T-Mobile Czech Republic a.s., která je součástí skupiny Deutsche Telekom (dále jen „DT“). Dodavatel je povinen opatření uvedená v této ISA uplatnit jako minimální bezpečnostní standard a tato opatření musí být uplatňována po celou dobu trvání Smlouvy a to i v případě, pokud jsou Plnění zajišťována na základě Smlouvy prostřednictvím třetích osob.

V ISA uvedená opatření pokrývají různé aspekty bezpečnosti informací a vztahují se na Plnění uvedená ve Smlouvě (v závislosti na povaze takových Plnění, jak je definováno níže).

Tato opatření mohou být navíc posílena o dodatečná bezpečnostní opatření, jež budou zajištěna Kupujícím a dohodnuta mezi Smluvními stranami v dokumentech přiložených ke Smlouvě, NPA a/nebo Objednávce, nebo jakoukoliv jinou související smlouvou, která takové bezpečnostní opatření bude řešit.

PRIORITA DOKUMENTŮ

ISA je standardní dokument, jenž se vztahuje na veškeré Smlouvy uzavřené s Dodavatelem, v nichž je uveden odkaz na ISA.

Platí následující:

1. Nebude-li ve Smlouvě stanoveno jiné pořadí priorit dokumentů, budou ustanovení Smlouvy nadřazena ustanovením ISA; a
2. Bez ohledu na výše uvedené, všechny výrazy psané s velkými počátečními písmeny budou vykládány v souladu s definicemi uvedenými na konci ISA a v souladu s definicemi ve Smlouvě odkazující na ISA.

Smluvní strany souhlasí, že ISA bude dále nadřazena dokumentům (politikám) Dodavatele, upravujícím bezpečnostní opatření, jež budou přílohou Smlouvy, NPA a/nebo Objednávky, případně na ně bude v těchto dokumentech odkazováno.

OBECNÁ PLATNOST ISA

Dodavatel je povinen dodržet požadavky ISA týkající se všech Plnění, jak je stanoveno níže:

- **Software** znamená komerčně dostupný dodavatelský software a/nebo individuálně vytvořený software vycházející ze Specifikace díla vzájemně dohodnuté mezi Smluvními stranami (např. Výsledný Software);
- **Hardware** včetně jakéhokoliv zabudovaného softwaru/firmwaru (např. koncová zařízení a přístroje pro Internet věcí - Internet of Things, IT vybavení);
- **XaaS/Cloud služby** (např. Software jako služba - Software as a Service);
- **Profesionální/Odborné služby** pro zajištění instalace, školení, integrace, údržby a/nebo poradenství;
- **Plnění Dodavatele, na které se vztahují požadavky Zákona o kybernetické bezpečnosti** v platném znění a představují plnění týkající se prvků a informačních systému, které jsou prvkem kritické infrastruktury Kupujícího a/nebo které přímo souvisí s dostupností, důvěrností a integritou provozu sítí a informačních systému Kupujícího jako osoby povinné podle zákona o kybernetické bezpečnosti (dále i „**Plnění týkající se kybernetické bezpečnosti**“)

OBECNÁ APLIKOVATELNOST JEDNOTLIVÝCH ČÁSTÍ S OHLEDEM NA PLNĚNÍ

Následující části se vztahují na všechny druhy Plnění zajišťovaného Dodavatelem:

- **Část A:** „Dodržování Smlouvy a norem (doporučených technických standardů)“
- **Část B:** „Organizace bezpečnosti“
- **Část C:** „Řešení incidentů“

Následující části se uplatní v závislosti na povaze Plnění, jak je definováno v tabulce A:

- **Část D:** „Šifrování a autentizace“
- **Část E:** „Záměrná bezpečnost (Security by design)“
- **Část F:** „Opravy softwarových Zranitelností ”
- **Část G:** „Data Kupujícího v: XaaS/Cloud službách, Plnění týkající se kybernetické bezpečnosti “
- **Část H:** „Řízení přístupu k: XaaS/Cloud službám, Plnění týkající se kybernetické bezpečnosti“
- **Část I:** „Provoz XaaS/Cloud služeb, Plnění týkající se kybernetické bezpečnosti“
- **Část J:** „Přístup k systémům a zdrojům Kupujícího a jejich využívání“
- **Část K:** „Odborní pracovníci a bezpečnost“

Plněni	Příslušné časti
Software	A, B, C, D, E, F
Hardware	A, B, C, D, E, F
XaaS / Cloud služby	A, B, C, D, E, F, G, H, I
Profesionální/Odborné služby	A, B, C, J, K
Plnění týkajíce se kybernetické bezpečnosti	A, B, C, D, E, F, G, H, I, J, K

Tabulka A: Aplikovatelnost částí ISA

NEDODRŽENÍ TÉTO ISA

Pokud Dodavatel v rámci svého Plnění zjistí jakoukoliv neshodu s bezpečnostními opatřeními uvedenými v této ISA, pak Dodavatel Kupujícímu neprodleně předloží analýzu situace a plán pro zajištění nápravy. Bude-li plán pro zajištění nápravy Kupujícím schválen, bude Dodavatelem implementován bez jakýchkoliv nákladů pro Kupujícího a Dodavatel poskytne důkaz o účinnosti plánu pro zajištění nápravy.

Pokud nedodržení požadavků přetrvává po dobu více než 30 dnů, nebude-li v konkrétním případě dohodnuta jiná lhůta a/nebo plán pro zajištění nápravy nebude schválen Dodavatelem nebo takový plán

nezajistí nápravu, bude takový stav automaticky považován za podstatné porušení Smlouvy, při tom Kupující je v takovém případě oprávněn odstoupit od Smlouvy.

A. DODRŽOVÁNÍ SMLOUVY A NOREM (DOPORUČENÝCH TECHNICKÝCH STANDARDŮ)

A.1 HODNOCENÍ BEZPEČNOSTI PLNĚNÍ

Na žádost Kupujícího poskytne Dodavatel Kupujícímu do 10 pracovních dnů všechny informace potřebné pro zhodnocení bezpečnosti Plnění, jako jsou zprávy o zkouškách/auditech bezpečnosti, kontroly zranitelnosti, či analýzy robustnosti kódu. Pokud Dodavatel poskytuje Kupujícímu Plnění tykající se kybernetické bezpečnosti, je povinen poskytovat Kupujícímu všechny potřebné informace, součinnost a spolupráci.

A.2. BEZPEČNOSTNÍ POLITIKY

Dodavatel musí mít zavedenu firemní politiku bezpečnosti informací, která svým obsahem odpovídá normě ISO/IEC 27001 nebo jinému podobnému standardu uznávaném v daném odvětví.

Je-li Dodavatel certifikován, musí Kupujícímu předložit svou bezpečnostní certifikaci a průběžně jej informovat o obnovení nebo odebrání svých certifikátů.

Pokud byl Dodavatel Kupujícím vybrán na základě určité certifikace (např. ISO/IEC 27001), pak je Dodavatel povinen takovou certifikaci udržovat po celou dobu plnění svých smluvních závazků.

A.3 AUDIT

Kupující je oprávněn provádět audity u Dodavatele s cílem ověřit dodržování bezpečnostních požadavků Kupujícího definovaných ve Smlouvě.

A.4 TŘETÍ OSOBY

V případě, že Dodavatel při poskytování Plnění Kupujícímu využívá třetí osoby, je Dodavatel povinen zajistit, aby tyto třetí osoby splňovali organizační a technické bezpečnostní opatření dohodnutá ve Smlouvě.

B. ORGANIZACE BEZPEČNOSTI

B.1 STRUKTURA

Na žádost Kupujícího je Dodavatel povinen poskytnout informace o organizaci své bezpečnosti, včetně systému řízení kybernetické bezpečnosti, pokud se tato povinnost Dodavatele týká.

B.2 KONTAKTNÍ MÍSTO

Dodavatel jmenuje kontaktní osobu pro bezpečnostní otázky, oznamování incidentů nebo jiných událostí a kontaktní osobu z řad vyššího vedení nebo Key Account Managera k řešení záležitostí eskalovaných z nižší úrovně. Kontaktní osoby budou zajištěny pro každé Plnění a jejich změny je nutné okamžitě sdělit Kupujícímu.

B.3 KONTROLY BEZPEČNOSTI

Jednou ročně, na žádost jedné nebo obou Smluvních stran, uspořádají Dodavatel a Kupující setkání, jehož cílem bude provést kontrolu bezpečnostních otázek (např. vývoj a plánované činnosti, jež mohou mít vliv na bezpečnost).

Každá Smluvní strana může požádat o mimořádné setkání v záležitostech týkajících se bezpečnosti, přičemž druhá Smluvní strana je povinna tento požadavek akceptovat v případech, kdy situace vyžaduje společnou analýzu nebo okamžité rozhodnutí (například v případě závažného incidentu nebo významného nárůstu hrozeb).

B.4 BEZPEČNOSTNÍ OPATŘENÍ PRO DATA KUPUJÍCÍHO

Dodavatel je povinen zavést následující opatření vztahující se k datům, která Kupující označí za důvěrná:

- všechna uložená a přenášená data musí být zašifrována;
- k zpracovávaným datům budou mít přístup jen oprávněné osoby;
- bude implementován silný autentizační systém (např. dvou-faktorová autentizace).

V případě nutnosti výměny zašifrovaných informací se smluvní strany předem dohodnou na způsobu jejich výměny.

Dodavatel je povinen zpracovávat data Kupujícího prostřednictvím zavedeného systému řízení identit a přístupových práv. Současně je Dodavatel povinen řídit všechny privilegované přístupy a výjimky z procesu řízení identit a přístupových práv.

C. ŘEŠENÍ INCIDENTŮ

C.1 ODHALOVÁNÍ

Dodavatel bude mít zavedená opatření pro detekci a řízení bezpečnostních incidentů, jež mají vliv na Kupujícího, a k nimž dojde v prostředí Dodavatele. Mezi bezpečnostní incidenty patří mimo jiné ztráta, změna, vyzrazení nebo neoprávněný přístup k datům či informacím Kupujícího a dále neoprávněné vyzrazení proprietárního zdrojového kódu a současně kybernetické bezpečnostní incidenty dle zákona o kybernetické bezpečnosti.

C.2 OZNAMOVÁNÍ

Dodavatel jakýkoliv bezpečnostní incident včetně veškerých skutečností majících vliv na zabezpečení kybernetické bezpečnosti bezodkladně oznámí Kupujícímu.

V případech, kdy dojde ke zjištění jakéhokoliv narušení a/nebo zneužití dat nebo informací Kupujícího, je Dodavatel povinen Kupujícího informovat bezodkladně v souladu s příslušnými právními předpisy.

Podrobnosti o bezpečnostních incidentech budou Dodavatelem uchovány v souladu s příslušnými právními předpisy, nejméně do příští bezpečnostní kontroly prováděné Smluvními stranami.

C.3 VYŘEŠENÍ

Dodavatel vynaloží veškeré úsilí k tomu, aby bezpečnostní incidenty ihned vyřešil a bude Kupujícího informovat o postupu a vyřešení incidentu včetně přijatých nápravných opatření.

C.4 POZASTAVENÍ PŘÍSTUPU DODAVATELE K SYSTÉMŮM KUPUJÍCÍHO

POZNÁMKA: Tento odstavec C.4 se nevztahuje na XaaS/Cloud služby.

V případě bezpečnostního incidentu může Kupující pozastavit přístup Dodavatele k systémům Kupujícího do doby, než bude incident vyřešen.

C.5 POZASTAVENÍ PŘÍSTUPU KUPUJÍCÍHO K XAAS/CLOUD SLUŽBÁM

POZNÁMKA: Tento odstavec C.5 se nevztahuje na Software, Plnění v oblasti Hardwaru a na Profesionální/Odborné služby a Plnění týkající se kybernetické bezpečnosti.

V případě bezpečnostního incidentu týkajícího se XaaS/Cloud služeb (např. průnik do systému, incident zahrnující malware) může Kupující pozastavit svůj přístup k uvedené Službě do doby, než bude incident vyřešen.

V případě, kdy Kupující nebude schopen přístup pozastavit, Kupující výslovně požádá Dodavatele o pozastavení veškerého přístupu Kupujícího až do doby vyřešení incidentu. Dodavatel takovému požadavku neprodleně vyhoví.

C.6 ZPRÁVA O BEZPEČNOSTI PRO XAAS/CLOUD SLUŽBY A ODBORNÉ SLUŽBY

Kupující může od Dodavatele požadovat předložení zprávy o bezpečnosti týkající se poskytovaných Plnění a to nejvíce dvakrát ročně; tím není dotčeno právo Kupujícího požadovat potřebné informace průběžně kdykoliv, pokud je to potřebné v souvislosti s plněním jeho zákonných povinností. Tato zpráva o bezpečnosti musí mimo jiné obsahovat následující informace:

- počet bezpečnostních incidentů zjištěných za posledních 12 měsíců, a to odděleně pro vnitřní a vnější příčiny, je-li toto rozdělení relevantní;
- podrobnosti o bezpečnostních incidentech v daném období (čas jejich odhalení, povaha a dopad, vyřešení, doba obnovy služeb, doba uzavření, čas nutný k vyřešení problému);
- všechny informace, které bude Kupující požadovat v souvislosti s plněním jeho zákonných povinností a požadavků, především v souvislosti s platnou legislativou v oblasti kybernetické bezpečnosti a ochrany soukromý.

D. ŠIFROVÁNÍ A AUTENTIZACE

D.1 ZMĚNA AUTENTIZAČNÍCH ÚDAJŮ A ŠIFROVACÍCH KLÍČŮ KUPUJÍCÍM

Veškeré autentizační údaje a šifrovací klíče (např. certifikáty, páry klíčů, symetrické klíče, hesla) v Plnění v oblasti Softwaru, Hardwaru a Plnění týkající se kybernetické bezpečnosti bude Kupující moci změnit a budou chráněny pomocí nejmodernějších (state-of-the-art) technologií. U autentizačních údajů a šifrovacích klíčů, které Kupující nemůže změnit, předloží Dodavatel Kupujícímu seznam takových údajů včetně informací o jejich účelu. V případě XaaS/Cloud služeb se tento požadavek vztahuje pouze na autentizační údaje využívané Kupujícím pro ochranu jeho dat.

D.2 SÍLA ŠIFROVACÍCH ALGORITMŮ A KLÍČŮ

Dodavatel implementuje pouze standardizované šifrovací algoritmy doporučované veřejnoprávními bezpečnostními autoritami (např. BSI, ANSSI a NIST) v době uzavření nebo prodloužení Smlouvy.

E. BEZPEČNOST NÁVRHU

E.1 ZVYŠOVÁNÍ ODOLNOSTI

Dodavatel u systémů uplatní standardní postupy pro zvyšování odolnosti (hardening). Tyto postupy zahrnují omezení protokolů pro přístup, odstranění nebo deaktivaci nepotřebného softwaru, síťových portů a služeb, odstranění nepotřebných souborů, uživatelských účtů, omezení oprávnění k souborům, správu záplat a protokolování.

Dodavatel poskytne Plnění (včetně součástí a služeb třetích osob), jež bude standardně (by default) bezpečně nakonfigurováno v souladu s nejmodernějšími (state-of-the-art) postupy pro konfiguraci bezpečnosti (jak jsou uvedeny například na stránkách https://www.cisecurity.org/).

Bez ohledu na výše uvedené platí, že Dodavatel poskytne Kupujícímu veškeré nezbytné informace pro bezpečnou konfiguraci a využití Plnění a zajistí, aby takové informace byly po celou dobu platnosti Smlouvy vždy aktuální.

Kromě toho je Dodavatel povinen zajistit, aby Plnění neobsahovalo žádná tzv. Zadní vrátka (Back doors).

E.2 TESTOVÁNÍ SOFTWARU S OHLEDEM NA BEZPEČNOSTNÍ CHYBY

Dodavatel je povinen provést testy Plnění s cílem zajistit, že Plnění nebude k datu předání obsahovat žádné nebezpečné softwarové chyby uvedené v „CWE/SANS Top 25“ (http://cwe.mitre.org) a/nebo v „OWASP TOP 10“ (http://www.owasp.org) (např. odolnost vůči neočekávaným vstupům, jako je SQL Injection, předvídatelnost chování v případech přetížení).

E.3. DODATEČNÁ OPATŘENÍ

Na žádost Kupujícího se mohou Smluvní strany navzájem dohodnout na dodatečných bezpečnostních opatřeních, která musí Plnění splňovat.

Tato dodatečná opatření mohou být uvedena v dokumentu nazvaném „Prohlášení o shodě v oblasti bezpečnosti“ (Security Statement of Compliance) a mohou být obsažena ve Smlouvě a/nebo v NPA.

F. OPRAVY ZRANITELNOSTÍ SOFTWARU

F.1 ODHALOVÁNÍ

Dodavatel zajistí přijetí takových opatření, jež umožní nepřetržité monitorování externích zdrojů bezpečnostních informací (jako jsou např. kooperační bezpečnostní testy, externí výzkum v oblasti bezpečnosti, open source a zjištění třetích osob) a bude sledovat Zranitelnosti, které by mohly mít vliv na Plnění (včetně součástí třetích osob).

F.2 CVE STANDARD

V případě potřeby bude každé Zranitelnosti zjištěné Dodavatelem přiřazen jedinečný identifikátor CVE spojený se skóre CVSS (verze 2 nebo vyšší). Jakákoliv alternativa musí být písemně schválena Kupujícím.

F.3 OZNÁMENÍ

Dodavatel neprodleně poskytne Kupujícímu informace o každé Zranitelnosti (se skóre CVSS vyšším nebo rovným 7,0), a to včetně Zero-Day s dopadem na Plnění a informací o případných důsledcích (např. případných CVE, skóre CVSS, dotčených komponent nebo služeb).

F.4 SMLOUVA O ÚROVNI SLUŽEB V SOUVISLOSTI S OPRAVOU ZRANITELNOSTÍ

Pro každou Zranitelnost, jež má vliv na Plnění, je Dodavatel povinen:

- poskytnout Kupujícímu Dočasnou opravu a Oficiální opravu v souladu s následující tabulkou.

Základní CVSS skóre v2	Maximální lhůta pro poskytnutí Dočasné opravy	Maximální lhůta pro poskytnutí Oficiální opravy
7,0-10,0	7 (sedm) kalendářních dnů	30 (třicet) kalendářních dnů
0-6,9	neuplatňuje se	6 (šest) měsíců

Měření této lhůty začíná v okamžiku zjištění Zranitelnosti – kromě Zranitelností souvisejících se součástmi Třetích osob, kde lhůta začíná běžet okamžikem, kdy je dostupná oprava.

F.5 ÚDRŽBA BEZPEČNOSTI SOUČÁSTÍ TŘETÍCH OSOB

Dodavatel zajistí, aby součásti Plnění poskytnuté třetími osobami, které byly použité v rámci Plnění na základě Smlouvy měly zajištěnou údržbu z hlediska bezpečnosti po celou dobu údržby nebo Služby nasmlouvané Kupujícím.

F.6 BEZPEČNOSTNÍ ZÁVADY

Dodavatel souhlasí s tím, že pro každou Zranitelnost ovlivňující Plnění, kterou Kupující v průběhu smluvní doby údržby a/nebo záruční doby zjistí, je Kupující oprávněn otevřít Požadavek na údržbu (maintenance ticket) s žádostí o její odstranění. Kromě odstavce 0 je Dodavatel povinen respektovat podmínky údržby a odstranit Závadu, která se Zranitelností souvisí.

F.7 VÝJIMKY

Dodavatel vynaloží komerčně přiměřené úsilí k tomu, aby Kupujícímu s odstraňováním Zranitelností pomohl:

- v situacích vyžadujících rychlejší reakci, než je uvedeno v tabulce výše (například při zveřejnění Zranitelnosti Plnění používaného Kupujícím prostřednictvím sdělovacích prostředků); a
- v technickém prostředí nezbytném pro provoz Plnění (např. v operačním systému v případě softwarového Plnění).

F.8 NÁHRADY ŠKODY/POKUTY ZA ODSTRANĚNÍ ZRANITELNOSTÍ

Kromě opravných postupů, jakož i nároků v případě podstatného porušení, jak je uvedeno v odstavci **Error! Reference source not found.** „**Error! Reference source not found.**“ výše, může Kupující vůči Dodavateli uplatnit nárok na náhradu škody a smluvní pokuty v souladu s ustanoveními Smlouvy upravujícími „Náhradu škody“ a „Smluvní pokuty“, jakož i v souladu s následujícím článkem:

V případě Zranitelností je Kupující oprávněn uplatnit následující smluvní pokuty:

Pokud Dodavatel neposkytne Oficiální opravu Zranitelnosti se skóre CVSS minimálním a vyšším než 7, jak je uvedeno v tabulce v části 0 „F.4 Smlouva o úrovni služeb v souvislosti s OPRAVOU ZRANITELNOSTÍ“, vypočítá se smluvní pokuta následovně:

A = V x N / 300

A: výše pokuty

V: hodnota příslušného Plnění

N: počet kalendářních dnů, o něž byl termín poskytnutí Oficiální opravy překročen

Pokuty uvedené v tomto odstavci F.8 jsou splatné do 30 kalendářních dnů od data doručení písemné výzvy k úhradě pokuty. Vznikem nároku na zaplacení pokuty, jejím vyúčtováním nebo zaplacením není dotčen nárok Kupujícího na náhradu veškeré újmy vzniklé ze stejného titulu, a to v plné výši. Pokuta může být Kupujícím započtena proti jakékoliv částce splatné Kupujícím Dodavateli na základě Smlouvy.

F.9 ÚDRŽBA SOUVISEJÍCÍ S BEZPEČNOSTÍ

V průběhu smluvní doby údržby a/nebo záruční doby je Dodavatel povinen poskytovat Plnění v oblasti Softwaru a Hardwaru a budoucí verze se všemi bezpečnostními záplatami (patch). Ty mohou být buď nainstalovány, nebo poskytovány současně ve formě samostatného balíku.

V průběhu životního cyklu Plnění je Dodavatel povinen poskytovat Kupujícímu bezpečností záplaty v době a v podobě, v jaké budou vydány, a to s respektováním lhůt pro Opravy Zranitelností definovaných v odstavci 0.

Dodavatel je povinen poskytnout Kupujícímu informace o Zranitelnostech (např. CVE, skóre CVSS), jež byly záplatami odstraněny.

G. DATA KUPUJÍCÍHO V XAAS/CLOUD SLUŽBÁCH, PLNĚNÍ TÝKAJÍCÍ SE KYBERNETICKÉ BEZPEČNOSTI

G.1 OMEZENÍ POUŽÍVÁNÍ DAT KUPUJÍCÍHO

Dodavatel bude data Kupujícího přenášet, zpracovávat, vytvářet a/nebo ukládat v XaaS/Cloud službě pouze za účelem poskytování uvedené Služby.

G.2 ODDĚLENÍ DAT KUPUJÍCÍHO

Dodavatel bude dbát na oddělení dat Kupujícího od dat jiných zákazníků Dodavatele.

G.3. DŮVĚRNÁ DATA KUPUJÍCÍHO

Všechna data, která budou Kupujícím klasifikována jako důvěrná, budou Dodavatelem pro přenos a uložení zašifrována.

G.4 ŠIFROVACÍ MECHANISMUS DODAVATELE

V případě, že Kupující využívá pro ochranu svých dat šifrovací mechanismus poskytnutý Dodavatelem, je Dodavatel povinen zajistit, aby:

- taková data byla v průběhu uložení a přenosu zašifrována; a
- pro přístup k takovým datům byla využívána silná autentizace (např. dvou-faktorová autentizace).

G.5 ZAZNAMENÁVÁNÍ (LOGOVÁNÍ) PŘÍSTUPU K DATŮM KUPUJÍCÍHO A JEJICH POUŽITÍ

Dodavatel zajistí:

- zaznamenávání (logování) přístupu k datům Kupujícího a jejich použití, a to včetně přístupů svých vlastních zaměstnanců a jakýchkoliv pověřených třetích osob;

- uchování takových záznamů (logů) po dobu dohodnutou v NPA a/nebo Objednávce včetně souvisejících dokumentů (např. ve Smlouvě o zachování mlčenlivosti nebo Smlouvě o zpracování dat), nebo standardně po dobu 6 měsíců.

Výpisy z uchovaných záznamů (logů) budou na vyžádání poskytnuty Kupujícímu.

G.6 VRÁCENÍ DAT KUPUJÍCÍMU

Po skončení Smlouvy nebo platnosti NPA a/nebo Objednávky vrátí Dodavatel Kupujícímu veškerá data Kupujícího, a to ve formátu a po dobu, na nichž se s Kupujícím předem dohodne.

V souladu s ustanoveními odstavce D.2 bude pro vrácení dat Kupujícímu použito výhradně šifrované připojení, nedá-li Kupující písemný souhlas s výjimkou z tohoto pravidla.

Na konci lhůty pro vrácení dat Dodavatel zlikviduje veškerá prostředí Kupujícího a to způsobem, jenž zaručí, že k žádným datům Kupujícího nebude nadále umožněn přístup a data nebude možné načíst.

Dodavatel poskytne Kupujícímu osvědčení o takovém zničení.

H. ŘÍZENÍ PŘÍSTUPU K XAAS/CLOUD SLUŽBÁM, PLNĚNÍ TÝKAJÍCÍ SE KYBERNETICKÉ BEZPEČNOSTI

H.1 FYZICKÁ BEZPEČNOST

Dodavatel je povinen zajistit prostory s odpovídající úrovní fyzického zabezpečení jak pro produkční cloud infrastrukturu, tak pro lokality pro vzdálené činnosti.

Opatření budou splňovat přinejmenším následující požadavky:

- fyzický přístup vyžaduje oprávnění a je monitorován;
- každý musí být při pohybu v prostorách viditelně opatřen oficiální identifikací;
- návštěvy se musí zapsat do knihy návštěv a musí být při pohybu v prostorách doprovázeny a/nebo sledovány;
- držení klíčů / přístupových karet a možnosti přístupu do lokalit jsou monitorovány;
- pracovníci, kteří ukončí pracovní poměr u Dodavatele, musí klíče/karty vrátit.

H.2 ŘÍZENÍ PŘÍSTUPU K SYSTÉMU A SPRÁVA HESEL

Dodavatel zajistí řízení přístupů do systémů pro poskytování Služeb, přičemž přístup bude omezen pouze na oprávněné pracovníky.

Dodavatel bude u součástí infrastruktury a systémů pro správu cloud, jež budou sloužit pro servisní prostředí Dodavatele, důsledně uplatňovat politiku hesel. Dodavatel zajistí ochranu hesel prostřednictvím bezpečných mechanismů, jako je například speciální nástroj pro ukládání hesel (digital vault).

Dodavatel zavede systematické řízení přístupu a jeho evidenci s cílem zajistit, aby přístup k systémům měli pouze schválení pracovníci provozu a podpory. Systematické řízení přístupu bude zahrnovat autentizaci, autorizaci, schválení přístupu, jeho poskytování a odebírání pro zaměstnance a jakékoliv další Dodavatelem definované „uživatele“.

H.3 KONTROLA PŘÍSTUPOVÝCH PRÁV

Účty pro zaměstnance Dodavatele v síti a v operačních systémech budou pravidelně kontrolovány tak, aby se zajistila odpovídající úroveň přístupových oprávnění pro příslušné zaměstnance.

V případě, že některý zaměstnanec Dodavatele smluvní projekt opustí, přijme Dodavatel urychlená opatření, aby ukončil síťový, telefonický a fyzický přístup takových bývalých zaměstnanců.

H.4 BEZPEČNOSTNÍ ROZHRANÍ (GATEWAY)

Dodavatel bude pro řízení přístupu mezi Internetem a Službami poskytovanými Dodavatelem používat bezpečnostní rozhraní (např. brány firewall, routery, servery proxy, reverzní servery proxy) které umožní pouze autorizovaný provoz.

Bezpečnostní rozhraní řízené Dodavatelem budou nasazeny tak, aby zajišťovaly kontrolu paketů, a budou u nich nastavena bezpečnostní pravidla pro filtrování paketů na základě protokolu, portu, zdrojové a cílové IP adresy (podle potřeby), aby bylo možné identifikovat oprávněné zdroje, cíle a typy provozu.

H.5 OPATŘENÍ PROTI MALWARE

Dodavatel bude využívat software na ochranu proti malware, jenž bude sloužit ke kontrole ukládaných souborů. Definice malware budou aktualizovány přinejmenším jednou denně.

H.6 ŠIFROVÁNÍ A VZDÁLENÝ PŘÍSTUP K XAAS/CLOUD SLUŽBÁM

Pro přístup Kupujícího ke XaaS/Cloud službě a pro její využívání musí být využito výhradně šifrované připojení, nedá-li Kupující písemný souhlas s výjimkou z tohoto pravidla.

Dodavatel zajistí, aby třetí osoby jednající jménem Dodavatele a využívající vzdálený přístup k datům Kupujícího zpracovávaným a/nebo uloženým v XaaS/Cloud službě využívaly pouze autentizované a šifrované připojení.

Ve všech případech musí být pro připojení k Xaas/Cloud službám podporovány nejnovější dostupné prohlížeče.

I. PROVOZ XAAS/CLOUD SLUŽEB, PLNĚNÍ TÝKAJÍCÍ SE KYBERNETICKÉ BEZPEČNOSTI

I.1 PENETRAČNÍ TESTY

Dodavatel bude provádět hodnocení bezpečnosti poskytovaných Plnění prostřednictvím penetračních testů, a to nejméně jednou ročně. Zpráva z hodnocení a plán zmírňování následků takových testů budou poskytnuty Kupujícímu.

Bez ohledu na výše uvedené platí, že Dodavatel umožní Kupujícímu provádění penetračních testů na své produkční prostředí.

I. 2 PRODUKČNÍ DATA A PROSTŘEDÍ

Dodavatel nebude pro testování využívat produkční data.

Dodavatel oddělí vývojové, testovací a produkční prostředí (sítě, data, aplikace atd.).

I.3 PLÁN OBNOVY PO HAVÁRII (DISASTER RECOVERY PLAN)

Dodavatel vytvoří a bude udržovat plán obnovy po havárii a zajistí, aby tento plán byl v pravidelných intervalech testován.

Zálohy budou Dodavatelem při likvidaci bezpečně smazány.

I.4 ÚDRŽBA SOUVISEJÍCÍ S BEZPEČNOSTÍ

V případě jakýchkoliv bezpečnostních záplat (patchů), které Dodavatel hodlá nasadit při poskytování Plnění, je Dodavatel povinen danou bezpečnostní záplatu nasadit a otestovat v testovacím prostředí. Teprve po úspěšném dokončení testů v testovacím prostředí může Dodavatel záplatu nasadit v produkčním prostředí.

I.5 SLUŽBY TŘETÍCH OSOB

Dodavatel je oprávněn při poskytování Plnění využívat služby třetí osoby (např. služby datového centra), pouze po předchozím písemném schválení Kupujícího.

J. PŘÍSTUP K SYSTÉMŮM A ZDROJŮM KUPUJÍCÍHO A JEJICH VYUŽITÍ

Tento odstavec se uplatní pouze v případech, kdy Kupující poskytne Dodavateli pro účely plnění Smlouvy přístup a umožní mu použití systémů Kupujícího.

J.1 FYZICKÝ PŘÍSTUP

Pokud Kupující poskytne přístup k vybavení a/nebo samotné vybavení pro připojení, které je/bude umístěné v prostorách Dodavatele, Dodavatel zajistí, aby:

- bylo v technickém prostoru, kde se takové zařízení nachází, uplatněno řízení fyzického přístupu;
- fyzický přístup k takovému zařízení byl omezen pouze na ty osoby, které přístup k takovému zařízení potřebují pro účely plnění Smlouvy a jsou Dodavatelem řádně proškoleny.

J.2 SYSTÉMY KUPUJÍCÍHO

Dodavatel pro jím řízené osoby zajistí:

- přístup k systémům Kupujícího a jejich používání výhradně za účelem poskytování Plnění;
- přístup a přenosy dat nebudou využívány pro provedení útoku (např. kontrola malware v rámci přenášených dat);
- dodržování způsobů přístupu a pravidel definovaných Kupujícím (včetně pravidel dobré praxe) a předem poskytnutých Dodavateli (např. bude respektovat síťové adresy přidělené Kupujícím, bude respektovat doby odezvy Kupujícího pro Zdroje řízení Kupujícího);
- řádnou autorizaci všech osob, které potřebují používat systémy Kupujícího včetně poskytnutí jejich identifikačních údajů Kupujícímu a průběžné aktualizace seznamu těchto (oprávněných) osob;
- připojení pouze řádně autorizovaných Zdrojů Dodavatele k systémům Kupujícího.

J.3 SYSTÉMY A APLIKACE KUPUJÍCÍHO

Pokud Kupující poskytne Dodavateli účty, je Dodavatel povinen:

- neprodleně Kupujícího informovat v případě, kdy daný uživatelský účet není nadále vyžadován;
- zajistit, aby účty poskytnuté pro serverovou komunikaci byly používány výhradně za tímto účelem.

J.4 ŘÍZENÍ A PROVOZ INFORMAČNO-KOMUNIKAČNÝCH TECHNOLOGIÍ KUPUJÍCÍHO

Pokud Dodavatel poskytuje Plnění týkajíce kybernetické bezpečnosti Kupujícího, je Dodavatel povinný:

- dodržovat pravidla přepojování systémů Kupujícího a přenosu elektronických informaci;
- řídit bezpečnost sítě a změn infrastruktury podle pravidel a pokynů Kupujícího;
- uplatnit řízení kapacit systémů a služeb podle pravidel a pokynou Kupujícího;
- využívat řádné kryptografické opatření; a
- mít implementovaný systém řízení kontinuity procesů a činností a zabezpečit soulad se systémem řízení kontinuity podnikání Kupujícího.

J.5 ŘÍZENÍ AKTIV KUPUJÍCÍHO

Pokud Kupující poskytne Dodavateli Aktiva Kupujícího, je Dodavatel povinen tato Aktiva Kupujícího evidovat a řídit přístup k nim za náležitého uplatnění klasifikace těchto Aktiv. Obdobný přístup Dodavatel uplatňuje i v případě zpracovaní osobních údajů zpřístupněných Kupujícím.

Po skončení Smlouvy je Dodavatel povinný vrátit Aktiva Kupujícího, které bude mít v tom čase ve své držbě. Současně je Dodavatel povinen po ukončení smluvního vztahu udělit, poskytnut, převést nebo postoupit všechny potřebné licence, práva nebo souhlasy nevyhnutné na zabezpečeni provozu Plnění na Kupujícího; tento závazek Dodavatele zůstává v platnosti i po ukončení smluvního vztahu nejméně po dobu pěti let po ukončení smluvního vztahu, pokud nebude dohodnuté jinak.

K. ODBORNOST PRACOVNÍKŮ A BEZPEČNOST

K.1 ŠKOLENÍ A VZDĚLÁVÁNÍ (AWARENESS)

Dodavatel je povinen zajistit, aby jeho zaměstnanci a jakékoliv třetí osoby pověřené poskytováním Plnění:

- disponovaly odpovídajícími schopnostmi v oblasti bezpečnosti (např. aby byly schopny řešit bezpečnostní incidenty);
- byly obeznámeny s obsahem a implementací příslušných bezpečnostních pravidel a všechny aktivity vykonávali podle těchto pravidel;
- dodržovaly mlčenlivost o veškerých skutečnostech a informacích Kupujícího a podepsaly prohlášení o zachování mlčenlivosti.

K.2 SPECIFICKÁ BEZPEČNOSTNÍ PRAVIDLA KUPUJÍCÍHO

Pokud Kupující stanoví specifická bezpečnostní pravidla pro poskytování Profesionálních/Odborných služeb a Plnění týkající se kybernetické bezpečnosti, je Dodavatel povinen zajistit, aby jeho zaměstnanci a pověřené třetí osoby byly před zahájením jakýchkoliv činností o takových pravidlech informovány.

K.3 SUBDODÁVKY

Využívá-li Dodavatel k plnění Smlouvy uzavřené s Kupujícím subdodavatele, může tak konat po předchozím souhlasu Kupujícího, musí ho výslovně označit jako subdodavatele a zabezpečit a smluvně zavázat, že bude z jejich strany vždy vynakládaná stejná řádná starostlivost.

K.4 PRÁCE S CITLIVÝM PLNĚNÍM

Na žádost Kupujícího se Dodavatel zavazuje využívat k práci s citlivým Plněním, než bude nasazeno v Síti Kupujícího, a dále k údržbě citlivého Plnění během celé provozní fáze pouze takové pracovníky, kteří prošli bezpečnostní prověrkou, tj. prověřené příslušnými státními orgány.

DEFINICE A ZKRATKY

Smlouva	znamená jakoukoliv smlouvu uzavřenou mezi Kupujícím a Dodavatelem, a která odkazuje na tuto ISA.
Aktiva	zahrnuje primární a podpůrná aktiva, jak jsou definována v ISO/IEC 27005.
Zadní vrátka („Back doors“)	znamená funkci nebo závadu Plnění, jež umožňuje skrytý neoprávněný přístup k datům.
CVE	znamená běžné zranitelnosti a rizika definovaná na: http://cve.mitre.org/index.html.
CVSS	znamená Common Vulnerability Scoring System (Systém hodnocení běžných zranitelností), jak je definován na: http://www.first.org/cvss/.
Závada	znamená jakoukoliv odchylku aktuální kvality Plnění od smlouvou zamýšlené kvality, např. neplnění, neshodu Plnění s jeho odpovídající specifikací nebo neschopnost Plnění fungovat v souladu s příslušnou dokumentací.
Plnění	znamená všechna zařízení, produkty a/nebo služby objednané podle hlavní Smlouvy, včetně všech hlavních nebo dodatečných závazků.
Bezpečnost informací	znamená – v souladu s ISO/IEC 27001 a ISO/IEC 27005 – bezpečnost v rozsahu zpracování informací a činností (primárních aktiv) spoléhajících na technické (včetně, mimo jiné, IT, prostor, zařízení a sítí) a netechnické zdroje (včetně, mimo jiné, podpůrných aktiv, jako např. personálu, partnerů, organizací, postupů, obchodních podmínek).
Internet věcí	znamená jakákoliv připojená zařízení nebo vybavení určená pro internet věcí.
NPA	znamená smlouvu uzavřenou s jakoukoliv sesterskou společností Kupujícího na základě Rámcové smlouvy, jež může být případně uzavřena. NPA odpovídá pojmům „Realizační smlouva“, „Smlouva pro konkrétní projekt“ a „Smlouva o projektu“: každé ustanovení využívající pojem „NPA“ se rovněž vztahuje na uvedené druhy smluv.
Oficiální oprava	znamená, že je dostupné kompletní řešení Dodavatele k opravě Zranitelnosti formou oficiální (řádné) záplaty (patche) nebo upgrade.
Objednávka	znamená nákupní objednávku vystavenou Kupujícím. „Objednávka“ odpovídá pojmu „Nákupní objednávka“ uváděnému ve Smlouvách uzavřených Kupujícím a jeho sesterskými společnostmi. Každé ustanovení používající pojem „Objednávka“ se obdobně vztahuje na „Nákupní objednávku“.
Kupující	znamená Kupujícího, jakož i jeho sesterskou společnost, která je smluvní stranou NPA nebo Objednávky. „Kupující“ odpovídá pojmu „Objednavatel“ uváděnému ve Smlouvách uzavřených Kupujícím a jeho sesterskými společnostmi. Každé ustanovení vztahující se na Kupujícího v této ISA se rovněž obdobně vztahuje na „Objednavatele“.
Síť Kupujícího	znamená síť spravovanou Kupujícím a veškerou související infrastrukturu pro přístup k Síti Kupujícího nezbytnou pro zajištění komunikace mezi zdroji jednotlivých stran.
Zdroje Kupujícího	znamená hardware, software, služby náležející Kupujícímu a používané za účelem poskytování Plnění.
Výsledný Software	znamená jakýkoliv software, který: (i) primárně vychází z požadavků Kupujícího a/nebo Specifikací poskytnutých Kupujícím nebo výhradně pro Kupujícího a/nebo který se těmito požadavky řídí a/nebo (ii) byl vyvinut nebo implementován Dodavatelem na základě této Smlouvy (a/nebo jakýchkoliv jejích pozdějších dodatků) a/nebo jakoukoliv NPA a/nebo Objednávku, a který není určen k běhu na pozadí; může nebo nemusí být chráněn právy z duševního vlastnictví, a dále jakékoliv produkty nebo procesy z něj vyplývající.
Prohlášení o shodě	znamená přílohu Smlouvy s podrobnými technickými bezpečnostními požadavky na Plnění.
Specifikace díla (Statement of Work - SoW)	znamená dokument definující specifické činnosti, plnění a časový harmonogram Dodavatele v souvislosti s poskytováním Plnění a/nebo Služeb Kupujícímu v rámci daného projektu.
Zdroje Dodavatele	znamená hardware, software patřící a/nebo v odpovědnosti Dodavatele, jež jsou využívány za účelem poskytování Plnění.
Dočasná oprava	znamená případ, kdy je dostupná oficiální (řádná), nicméně dočasná oprava Zranitelnosti, včetně, mimo jiné, dočasných hotfixes, nástrojů nebo dočasných řešení (workaround).
Zranitelnost	znamená slabinu snižující dostupnost, integritu nebo důvěrnost informací.

XaaS	znamená cokoliv, co je uživatelům poskytováno jako služba, včetně SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) či podobné.
Nultý den (Zero-Day)	znamená dosud nezjištěnou zranitelnost, kterou mohou hackeři využít pro nepříznivé ovlivnění Plnění. Tato zranitelnost známa pod názvy „zero-day“ (nebo „zero-hour“ nebo „0-day“ nebo „day zero“ nebo „zranitelnost nultého dne“), nebyla do jejího využití veřejně známa či oznámena, což znamená, že Kupující je ohrožen a až do vydání opravy (aktualizace) se nachází ve výchozím postavení (tj. v nultém dni) a Dodavatel musí vytvořit záplatu nebo doporučit dočasné řešení (workaround) pro zmírnění jejího dopadu.

PŘÍLOHA Č. 2 – BCM POŽADAVKY

1) Pro zajištění ochrany podnikání TMCZ je Dodavatel povinen zavést a udržovat účinný systém kontinuity podnikání ve shodě s ISO 22301. Tento systém musí zahrnovat i pravidelné testování plánů kontinuity činností pro ujištění, že v případě mimořádné nebo krizové situace a bezprostředně po ní bude Dodavatel schopen pokračovat v plnění závazků vůči TMCZ.
2) Dodavatel zajistí dostatečnou míru odolnosti a obnovitelnosti předmětu dodávky tak, aby bylo zaručeno dosažení cílů doby zotavení (RTO), jak jsou ustanoveny v dohodě o úrovni poskytovaných služeb (SLA) pro každou poskytovanou službu.
3) Během tzv. přechodové fáze kontraktu prokáže Dodavatel svoji schopnost obnovy všech dodávaných služeb vytvořením příslušné dokumentace, která bude následně testována z pohledu přesnosti a úplnosti.
4) Dodavatel zavede a bude udržovat systém řízení rizik (včetně identifikace rizik, jejich kontroly a procesu akceptace) pro dodávané služby a relevantní platformy.
5) Dodavatel oznámí bezodkladně TMCZ zjištěná nebo potenciální rizika relevantní pro dodávanou službu.
6) Dodavatel poskytne TMCZ seznam známých rizik, vztahujících se ke všem aktivům relevantním pro dodávanou službu.
7) Dodavatel provádí analýzu dopadů (BIA) pro poskytované služby a platformy a identifikuje dopady a zranitelnosti podle metodiky dohodnuté s TMCZ.
8) Dodavatel je zodpovědný za tvorbu Business Continuity plánů, Disaster Recovery plánů a krizového plánu nebo obdobného dokumentu. TMCZ má právo nahlížet do této dokumentace.
9) Dodavatel je odpovědný za vytváření, údržbu a testování dokumentace BCM v rozsahu dodávaných služeb a platforem. TMCZ bude v této oblasti s Dodavatelem spolupracovat.
10) Dodavatel bude provádět revize BCM dokumentace v pravidelných intervalech a s každou významnou změnou, nejméně však jedenkrát za 2 roky. Změny budou podléhat schvalování TMCZ.
11) Dodavatel zajistí udržování povědomí svých příslušných zaměstnanců o obsahu dokumentace BCM k předmětu dodávky, prověřuje správné pochopení obsahu dokumentace a provádí pravidelná školení a aktualizace.
12) Dodavatel zajistí dostatek vyškolených zaměstnanců v pohotovosti pro případ řešení mimořádné události.
13) TMCZ ověří připravenosti Dodavatele splnit závazky z BCM pomocí pravidelných cvičení.
14) Dodavatel bude provádět testování zavedených opatření systému kontinuity podnikání podle požadavků smlouvy minimálně 1x za 3 roky.
15) Dodavatel bude spolupracovat s TMCZ při dohodnutých cvičeních BCM.
16) Dodavatel bude informovat nejméně jeden měsíc dopředu TMCZ, pokud bude připravovat cvičení BCM a po ukončení cvičení předá TMCZ zprávu o výsledcích cvičení.
17) TMCZ si vyhrazuje právo provést audit systému kontinuity podnikání u Dodavatele. TMCZ akceptuje i audit nezávislé auditní autority, pokud se vztahuje k předmětu dodávky.
18) TMCZ si pro ověření funkčnosti plánů obnovy Dodavatele vyhrazuje právo účastnit se jeho Disaster Recovery cvičení.
19) TMCZ si vyhrazuje právo nahlížet do BCM dokumentace dodavatele.
20) Dodavatel neprodleně oznámí TMCZ identifikační údaje outsourcing partnera, jestliže předmět dodávky, nebo jeho části budou outsourcovány.
21) Dodavatel bude po svých kritických dodavatelích požadovat alespoň stejnou míru zajištění kontinuity činností, jako TMCZ požaduje po něm.
22) Dodavatel provede bezodkladně (nejdéle však do 3 měsíců) implementaci nutných opatření, definovaných auditem, nebo vzešlých z testů, cvičení, poruch, analýzy rizik, nebo procesu řízení změn, týkající se předmětu dodávky.
23) Dodavatel poskytne TMCZ informace a nálezy z auditu ISO 27001 a 22301, zvláště pak zjištění týkající schopnosti Dodavatele poskytovat předmět dodávky.
24) Dodavatel neprodleně nahlásí TMCZ všechny bezpečnostní incidenty, které způsobily, nebo mohou způsobit výpadek předmětu dodávky.
25) Dodavatel a TMCZ si dohodnou pravidla a požadavky na řešení incidentů.

PŘÍLOHA Č. 3 – SCHVÁLENÍ SUBDODAVATELÉ

Obchodní firma (IČO, adresa, zápis v OR)	Poskytované služby	Zavedený/certifikovaný systém podle bodu 2 Pravidel
		Ano / Ne