Korporátne pravidlá informačnej bezpečnosti a ochrany dát

1. *Dodávateľ sa zaväzuje pri poskytovaní plnenia podľa Zmluvy dodržiavať požiadavky nasledujúcich medzinárodných štandardov ako vyplýva z nasledujúcej tabuľky:*

Systém:
Systém managementu kvality podľa ISO 9001
Systém environmentálneho managementu podľa ISO 14001
Systém managementu bezpečnosti informácií podľa ISO 27001
Systém riadenia kontinuity podľa ISO 22301
Systém manažmentu služieb v informačných technológiách podľa ISO 20000-1

2. *Dodávateľ sa zaväzuje poskytovať plnenie podľa Zmluvy a zabezpečovať výkon činností, ku ktorým sa zaviazal podľa Zmluvy primárne prostredníctvom svojich kmeňových zamestnancov. Dodávateľ nie je oprávnený poveriť výkonom svojich povinností podľa Zmluvy žiadneho subdodávateľa bez predchádzajúceho súhlasu spoločnosti Slovak Telekom, a.s. (ďalej ST) / T-Mobile Czech Republic a.s. (ďalej TMCZ). Dodávateľ môže o takýto súhlas požiadať zaslaním žiadosti na email: security@telekom.sk, kde priloží vyplnený dokument, ktorý je uvedený v prílohe č.3 dokumentu Korporátne pravidlá informačnej bezpečnosti a ochrany.*

3. *Ak ST/TMCZ udelí Dodávateľovi súhlas s použitím konkrétneho subdodávateľa, je Dodávateľ povinný uzavrieť so subdodávateľom zmluvu, ktorá zabezpečí, aby subdodávateľ vykonával povinnosti podľa Zmluvy za rovnakých podmienok a za rovnakej kvality, ako je medzi ST/TMCZ a Dodávateľom dohodnuté v Zmluve tak, aby bolo zabezpečené dodržanie požiadaviek ST/TMCZ definovaných Zmluvou. Dodávateľ je plne zodpovedný za riadne a včasné plnenie týchto povinností subdodávateľom. Predovšetkým, ale nie výlučne, sa takýto subdodávateľ musí zaviazať k dodržiavaniu ustanovení dokumentu Korporátne pravidlá informačnej bezpečnosti a ochrany dát Zmluvy. Osobitne musia byť zmluvne ošetrené so subdodávateľom podmienky pre prístup, práva a povinnosti pre zabezpečenie ochrany Chránených informácií.*

4. *V prípade, že Dodávateľ má zavedený alebo certifikovaný systém, ako je popísaný v bode 1. vyššie, potom je povinný predložiť ST/TMCZ k nahliadnutiu a kontrole dokumentované informácie (napr. dokumenty, záznamy, logy, nahrávky) súvisiace s požiadavkami vyššie popísaných systémov, a to za účelom preukázania súladu s požiadavkami definovanými horeuvedenými medzinárodnými štandardami, ako aj Zmluvou. V prípade, že Dodávateľ poskytuje plnenie podľa Zmluvy pomocou a/alebo prostredníctvom schválených subdodávateľov, ktorí majú niektorý zo systémov zavedený či certifikovaný, zabezpečí Dodávateľ súhlas s vykonaním auditov aj u týchto subdodávateľov a to za účelom preverenia zhody s predmetnými normami.*

5. *V prípade, že Dodávateľ nemá niektorý systém certifikovaný ani zavedený, súhlasí s vykonaním auditov zameraných na preverenie zhody s požiadavkami Zmluvy. Dodávateľ je povinný poskytnúť zamestnancom ST / TMCZ alebo splnomocneným osobám pri výkone auditu alebo pri analýze rizík súčinnosť, predložiť k nahliadnutiu a na kontrolu dokumentované informácie (napr.: dokumenty, záznamy, logy, nahrávky), umožniť prístup do priestorov a systémov súvisiacich s plením podľa Zmluvy. V prípade, že Dodávateľ poskytuje plnenie podľa tejto zmluvy za pomoci a / alebo prostredníctvom schválených subdodávateľov, ktorí nemajú niektorý zo systémov zavedený či certifikovaný, zaistí Dodávateľ súhlas s vykonaním auditu aj u týchto subdodávateľov a to za účelom preverenia zhody so Zmluvou.*

6. *Dodávateľ a jeho subdodávateľia musia v dohodnutých termínoch vykonať aktivity a/alebo implementovať nápravné opatrenia, ktoré boli identifikované a dohodnuté ako výstup auditov Dodávateľa. Rovnako sú povinní vykonať aktivity a implementovať nápravné opatrenia identifikované napr. pri testoch, cvičeniach, incidentoch, riadení rizík. Dodávateľ poskytne ST/TMCZ všetky informácie (napr. správy z auditov), ktoré sa týkajú schopnosti Dodávateľa poskytovať plnenie podľa Zmluvy ST/TMCZ. Ak implementácia nápravných opatrení bude trvať po dobu dlhšiu než 30 dní, ak nebude v konkrétnom prípade dohodnutá iná lehota a / alebo plán pre zaistenie nápravy nebude schválený Dodávateľom alebo takýto plán nezabezpečí nápravu, bude taký stav automaticky považovaný za podstatné porušenie zmluvy.*

7. *Dodávateľ musí mať zavedený systém riadenia kontinuty činností, aby bol schopný ST/TMCZ poskytovať plnenie podľa Zmluvy v prípade neštandardných a neočakávaných situáciách nepretržite a v súlade s parametrami a kvalitou dohodnutou medzi zmluvnými stranami. Dodávateľ je povinný poskytnúť ST/TMCZ súčinnosť pri príprave a realizácii plánov kontinuity činností alebo obnovy po havárii v ST/TMCZ. Dodávateľ je povinný pri poskytovaní plnenia podľa Zmluvy dodržiavať požiadavky na riadenie kontinuity činností uvedené v prílohe č. 2 dokumentu Korporátne pravidlá informačnej bezpečnosti a ochrany dát Zmluvy za predpokladu že plnenie podľa Zmluvy bude vyhodnotené z BIA ako kritické a / alebo existuje zákonný dôvod pre riadenie Dodávateľa v oblasti riadenia kontinuity činností (BCM).*

8. *Dodávateľ je povinný nakladať s odpadmi, ktorých je pôvodca alebo vlastníkom, v súvislosti s plnením podľa Zmluvy, v súlade so všeobecne záväznými právnymi predpismi upravujúcimi oblasť odpadov.*

9. *Zamestnanci, delegované osoby a subdodávateľia (ďalej Poverené osoby) Dodávateľa vstupujúce do priestorov a objektov ST/TMCZ a vykonávajúce tam činnosť podľa Zmluvy, sú povinné zoznámiť sa s dokumentáciou BOZP, OPP a požiarno-technickými zariadeniami umiestnených v priestoroch objektu.*

10. *Dodávateľ sa zaväzuje v súlade s platnými predpismi o ochrane pred požiarmi:*
    a) *dodržiavať platné a záväzné predpisy o ochrane pred požiarmi;*
    b) *dodržiavať pravidlá požiarnej bezpečnosti stanovené v Prevádzkových predpisoch objektov a priestorov ST*
    c) *zabezpečiť účasť Poverených osôb na školeniach o ochrane pred požiarmi, pokiaľ sa jeho Poverené osoby zdržujú v objektoch a priestoroch ST;*

11. *Zmluvná strana sa zaväzuje dodržiavať všetky právne predpisy a ostatné predpisy na zaistenie bezpečnosti a ochrany zdravia pri práci.*

12. *Zmluvné strany berú na vedomie a súhlasia s tým, že všetky informácie obsiahnuté v Zmluve ako aj v nadväzujúcich zmluvách a informácie vymieňané medzi zmluvnými stranami v súvislosti s poskytovaním plnenia podľa Zmluvy, budú považované za dôverné a chránené v rozsahu podmienok dohodnutých v zmluve o dôvernosti uzavretej medzi zmluvnými stranami (ďalej len ako "NDA"). Zmluvné strany berú na vedomie a súhlasia s tým, že v prípade odlišných ustanovení NDA a Zmluvy, majú prednosť ustanovenia Zmluvy.*

13. *Pokiaľ nie je uvedené inak, každá Zmluvná strana sa zaväzuje vytvoriť, používať a udržiavať primerané technické, organizačné a personálne bezpečnostné opatrenia na zaistenie dôvernosti, dostupnosti a integrity Chránených informácií. Tieto opatrenia musia byť dostatočné, aby sa zabránilo náhodnému*

alebo neoprávnenému zničeniu, strate, zámene, sprístupneniu údajov alebo akýmkoľvek neoprávneným formám využívania Chránených informácií. Zmluvné strany sú povinné udržiavať tieto opatrenia vo funkčnom stave počas celého obdobia využívania Chránených informácií.

14. *Pri poskytovaní plnenia podľa Zmluvy je Dodávateľ zodpovedný za to, že plnenie bude dodané bez vád, s náležitou starostlivosťou a v súlade s prílohou č. 1 dokumentu Korporátne pravidlá informačnej bezpečnosti a ochrany dát Zmluvy.*

15. *Dodávateľ prehlasuje, že plnenie podľa Zmluvy budú jeho menom dodané iba prostredníctvom zamestnancov, ktorí sú vo vzťahu k charakteru plnenia bezúhonní a spĺňajúci potrebné kvalifikačné predpoklady a že je preto schopný na vyžiadanie ST/TMCZ preukázať. Táto povinnosť platí obdobne pre subdodávateľov, ktorí sa menom Dodávateľa budú podieľať na poskytovaní plnenia.*

16. *Dodávateľ berie na vedomie a poučí svojich Zamestnancov a subdodávateľov, že sú povinní najmä:*
    a) *pre vstup a výstup do a z priestorov ST/TMCZ používať výhradne hlavný vchod; ostatné vchody a východy môžu využiť len vo výnimočných situáciách (napr .: evakuácie, prínos či odnos nadmerného nákladu);*
    b) *tam, kde je vyžadované, preukázať sa bez vyzvania pri vstupe do priestorov príslušnému zamestnancovi a / alebo poverenej osobe;*
    c) *dbať, aby údaje (ak sú požadované) uvedené na prístupovom prostriedku zodpovedali skutočnosti;*
    d) *chrániť Prístupový prostriedok pred poškodením, zničením, stratou, krádežou a zneužitím inou osobou;*
    e) *neposkytovať Prístupový prostriedok iným osobám;*
    f) *ak bol pridelený, tak viditeľne nosiť preukaz návštevníka po celú dobu pobytu v priestoroch ST/TMCZ;*
    g) *bezodkladne oznámiť ST/TMCZ stratu, krádež, poškodenie, zneužitie Prístupového prostriedku, ako aj o zmenách údajov obsiahnutých na Prístupovom prostriedku;*
    h) *na vyzvanie zamestnanca ST/TMCZ sa preukázať Prístupovým prostriedkom;*
    i) *neumožniť vstup do objektu ST/TMCZ žiadnej osobe;*
    j) *po ukončení zmluvnej činnosti vrátiť Prístupový prostriedok, ako aj všetky ďalšie veci patriace ST/TMCZ.*

17. *Dodávateľ a všetky osoby podieľajúce sa na poskytovaní plnenia podľa Zmluvy v jeho mene, sú povinní podriadiť sa a rešpektovať zavedené bezpečnostné opatrenia ST/TMCZ a bezpečnostné pokyny a nie sú oprávnení vykonávať žiadne činnosti, ktoré by mohli tieto opatrenia narušiť alebo poškodiť.*

18. *Dodávateľ je povinný zabezpečiť ochranu dôvernosti a integrity Prístupových prostriedkov (prístupové ID, heslá, tokeny čipové karty, vstupné karty, kľúče a pod.) do elektronických systémov a priestorov ST/TMCZ, ktoré sú Dodávateľovi sprístupnené na základe Zmluvy a / alebo čiastkovej zmluvy či objednávky a nesmie ich sprístupniť tretím osobám. Dodávateľ je povinný bezodkladne oznámiť ST/TMCZ stratu, krádež, zneužitie alebo zničenie Prístupového prostriedku v súlade s čl. 21 dokumentu Korporátne pravidlá informačnej bezpečnosti a ochrany dát Zmluvy.*

19. *Dodávateľ je vždy povinný informovať ST/TMCZ pokiaľ niektorá z poverených osôb ukončí svoj pracovný (dodávateľský) vzťah s Dodávateľom a vrátiť všetky poskytnuté Prístupové prostriedky, ktoré ST/TMCZ tejto osobe poskytol. Stratený Prístupový prostriedok je Dodávateľ povinný ST/TMCZ nahradiť.*

20. *Chránené údaje s veľkým objemom budú medzi Zmluvnými stranami vymieňané výlučne spôsobom, ktorý zaručí dôvernosť a integritu prenášaných údajov (napr. prenosom pomocou SFTP protokolu súbormi, ktoré majú stanovený dohodnutý typ a format).*

21. *Zmluvné strany zriadia bod kontaktu pre riešenie všetkých problémov, vzájomné poskytovanie informácií, spoluprácu v oblasti bezpečnosti informácií a ochrany dát a určia kontaktnú osobu. Kontaktné informácie tejto osoby (meno, priezvisko, prac.pozícia, prac. e-mail a prac.tel.číslo) zašlú do 10 dní od podpisu zmluvy/akceptácie objednávky na email: security@telekom.sk. V prípade zmeny tejto osoby sa Zmluvná strana zaväzuje bezodkladne určiť novú kontaktnú osobu a oznámiť ST/TMCZ jej kontaktné informácie.*

22. *Dodávateľ je povinný bezodkladne ohlásiť ST/TMCZ akúkoľvek neštandardnú situáciu, podozrivé udalosti, bezpečnostné incidenty a stratu Prístupového prostriedku a to prostredníctvom nasledujúcich konktaktov:*
    a) pre ST: email: security@telekom.sk, tel .: +421 800 100 166
    b) pre TMCZ: email: security@t-mobile.cz, tel .: +421 800 100 166.
    Dodávateľ je povinný v rámci spolupráce s ST/TMCZ vynaložiť maximálne úsilie, aby zabránil pokračovaniu bezpečnostného incidentu, predišiel ďalším bezpečnostným incidentom, zaistil a obnovil všetky opatrenia potrebné na ochranu dát a informácií ST/TMCZ.

23. *Pokiaľ bude pri poskytovaní plnenia podľa tejto Zmluvy dochádzať k vykonávaniu činností priamo súvisiacich s prevádzkou sietí a informačných systémov pre ST ako prevádzkovateľa základnej služby podľa Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, v takom prípade sa Dodávateľ zaväzuje pred začatím vykonávania týchto činností uzatvoriť s ST osobitnú zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa § 19 ods. 2 Zákona 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.*

24. *Za porušenie dokumentu Korporátne pravidlá informačnej bezpečnosti a ochrany dát Zmluvy má ST/TMCZ právo na zmluvnú pokutu vo výške 100 000 EUR (slovami: sto tisíc). Zmluvná pokuta je splatná na základe vystavenej faktúry ST/TMCZ bez zbytočného odkladu po porušení zmluvných povinností, a to do 14 dní od jej vystavenia. Dodávateľ sa zaväzuje, že zmluvnú pokutu zaplatí riadne a včas. Uhradením zmluvnej pokuty nezaniká právo ST/TMCZ na náhradu škody v plnom rozsahu.*

25. *Dodávateľ je povinný zabezpečiť, aby ním Poverené osoby dodržiavali platné režimové, technické a organizačné opatrenia upravujúce riadenie vstupu, pohybu osôb a dopravných prostriedkov v priestoroch a objektoch ST/TMCZ. Pre umožnenie vstupu osôb a/alebo vjazd dopravných prostriedkov do priestorov a objektov ST/TMCZ bude Dodávateľovi vydané potrebné povolenia vydané príslušným oddelením ST/TMCZ. Dodávateľ si o povolenie požiada prostredníctvom konktaktnej osoby podľa bodu 21 dokumentu Korporátne pravidlá informačnej bezpečnosti a ochrany dát Zmluvy.*

26. *Za zoznámenie poverených osôb Dodávateľa s relevantnými internými predpismi ST/TMCZ, odovzdanie Prístupových prostriedkov určených pre Poverené osoby zodpovedá zodpovedná osoba ST/TMCZ.*

27. *Dodávateľ berie na vedomie, že ním Poverené osoby sa podrobia kontrole vykonávanej v súlade s internými predpismi ST/TMCZ (napr .: fyzická kontrola osôb a dopravných prostriedkov, technická*

kontrola zariadenia) pri vstupe do priestorov ST/TMCZ. Poverené osoby, ktoré vykonávajú činnosť v priestoroch ST/TMCZ sú povinné sa pred vstupom do týchto priestorov identifikovať (napr.: zamestnaneckým preukazom, preukazom totožnosti, občianskym preukazom, cestovným pasom).

28. *V prípade, že Dodávateľovi budú odovzdané Prístupové prostriedky do priestorov či objektov ST/TMCZ, je Dodávateľ povinný dodržiavať interné predpisy ST/TMCZ týkajúce sa Prístupových prostriedkov. Dodávateľ nesmie vyhotoviť duplikát alebo kópiu z prevzatého Prístupového prostriedku.*

29. *Dodávateľ a ním Poverené osoby sú oprávnené pri výkone plnenia podľa tejto zmluvy zdržiavať sa a pohybovať sa v priestoroch a objektoch ST/TMCZ len v čase potrebnom pre uskutočnenie zmluvne dohodnutých činností a služieb a len v priestoroch a objektoch, ktoré sú pre tieto činnosti určené.*

30. *Dodávateľ je povinný zabezpečiť, aby zdrojový kód, ktorý dodá v rámci spolupráce, obsahoval len kód vyvinutý v súlade s požiadavkami Zmluvy, bezpečnostnú dokumentáciu ST/TMCZ a v súlade s aplikovateľnými štandardmi podľa bodu 1. Dodávateľ sa najmä zaväzuje, že zdrojový kód nebude obsahovať žiadne zlomyseľné a/alebo škodlivé prvky či bezpečnostné slabiny umožňujúce narušenie bezpečnosti predmetu zmluvy, a že nebude obsahovať žiadny Mallware. Prístup k zdrojovému kódu bude Dodávateľ riadiť, obmedzovať na nevyhnutný okruh poverených osôb a chrániť proti neoprávnenej manipulácii.*

31. *Mallwarem sa rozumie najmä akýkoľvek počítačový program, súbor príkazov a inštrukcií použitých priamo alebo nepriamo v počítači so schopnosťou poškodiť, zasahovať, narušiť a / alebo akokoľvek nepriaznivo ovplyvniť softvéry, počítačové programy, dátové súbory a / alebo činnosť akéhokoľvek hadwaru, mobilných a iných koncových zariadení a / alebo sieťových funkcionalít vrátane vírusov, červov (worms), trójskych koní (trojan horse), spyware, zadných vrátok (back doors) a iných programov, ktoré úmyselne uskutočňujú akékoľvek zbytočné, narušujúce a / alebo ničivé funkcie v rámci informačného systému.*

32. *Zmluvná strana sa zaväzuje zabezpečiť:*
    a) *že pre vývojové a testovacie účely použije samostatne vyvinuté testovacie anonymizované dáta,*
    b) *samostatné vývojové a testovacie prostredie oddelené od živého prevádzkového systému,*
    c) *bezodkladnú bezpečnú preukázateľnú likvidáciu testovacích dát po skončení potreby ich použitia,*
    d) *pred odovzdaním plnenia podľa tejto Zmluvy do prevádzky akceptačné testy, ktorých súčasťou sú aj bezpečnostné testy.*

Príloha č. 1 - Príloha o bezpečnosti informácií

ISA_v3.doc

Príloha č. 2 - BCM požiadavky

BCM Požiadavky.c

Príloha č. 3 –Subdodávatelia

Schvaleni

Príloha č. 1

Príloha o bezpečnosti informácií

VŠEOBECNÉ ZÁSADY

Táto Príloha o bezpečnosti informácií (Information Security Annex, ďalej len "ISA") stanovuje opatrenia v oblasti bezpečnosti informácií v spoločnosti Slovak Telekom, a.s., ktorá je súčasťou skupiny Deutsche Telekom (ďalej len "DT"). Dodávateľ je povinný opatrenia uvedené v tomto ISA uplatniť ako minimálne bezpečnostné štandardy a tieto opatrenia musia uplatňované po celú dobu trvania zmluvy a to aj v prípade ak je Plnenie zabezpečované na základe zmluvy prostredníctvom tretích osôb.

V ISA uvedené opatrenia pokrývajú rôzne aspekty bezpečnosti informácií a vzťahujú sa na Plnenia uvedené v Zmluve (v závislosti od povahy takých Plnení ako je definované nižšie).

Tieto opatrenia môžu byť navyše posilnená o dodatočné bezpečnostné opatrenia, ktoré budú zaistené Kupujúcim a dohodnuté medzi Zmluvnými stranami v dokumentoch priložených k Zmluve, NPA a/alebo Objednávke.

PRIORITA DOKUMENTOV

ISA je štandardný dokument, ktorý sa vzťahuje na všetky zmluvy uzatvorené s Dodávateľom, v ktorých je uvedený odkaz na ISA.

Platí nasledujúce:

1. Ak nebude v Zmluve stanovené iné poradie priorít dokumentov, budú mať ustanovenia zmluvy prednosť pred ustanoveniami ISA; a
2. Bez ohľadu na vyššie uvedené, všetky výrazy písané s veľkými písmenami sa budú vykladať v súlade s definíciami uvedenými na konci ISA a v súlade s definíciami v Zmluve odkazujúce na ISA.

Zmluvné strany súhlasia, že ISA bude ďalej nadradená dokumentom (politikám) Dodávateľa, upravujúcim bezpečnostné opatrenia, ktoré budú prílohou Zmluvy, NPA a / alebo Objednávky, prípadne na ne bude v týchto dokumentoch odkaz.

VŠEOBECNÁ PLATNOSŤ ISA

Dodávateľ je povinný dodržať požiadavky ISA týkajúce sa všetkých Plnení, ako je stanovené nižšie:

- **Softvér** znamená komerčne dostupný dodávateľský softvér a / alebo individuálne vytvorený softvér vychádzajúci zo Špecifikácie diela vzájomne dohodnuté medzi Zmluvnými stranami (napr. Výsledný Software);
- **Hardware** vrátane akéhokoľvek zabudovaného softwaru / firmware (napr. Koncové zariadenia a prístroje pre Internet vecí (Internet of Things), IT vybavenie);
- **XaaS / Cloudové služby** (napr. Softvér ako služba (Software as a Service)); a
- **Profesionálne služby** pre zaistenie inštalácie, školenia, integrácie, údržby a / alebo poradenstvo.

VŠEOBECNÁ APLIKOVATEĽNOSŤ JEDNOTLIVÝCH ČASTÍ S OHĽADOM NA PLNENIE

Nasledujúce časti sa vzťahujú na všetky druhy Plnení zabezpečovaného Dodávateľom:

- **Časť A:** "Dodržiavanie zmluvy a noriem (Odporúčaných technických štandardov) "
- **Časť B:** "Organizácia bezpečnosti"
- **Časť C:** "Riešenie incidentov"

Nasledujúce časti sa uplatnia v závislosti od povahy Plnenia, ako je definované v tabuľke A:

- **Časť D:** "Šifrovanie a autentizácia"
- **Časť E:** "Zámerná bezpečnosť (Security by design)"
- **Časť F:** "Opravy softvérových Zranitelností"
- **Časť G:** "Dáta Kupujúceho v XaaS / cloudových službách"
- **Časť H:** "Riadenie prístupu k XaaS / cloudovým službám"
- **Časť I:** "Prevádzka XaaS / cloudových služieb"
- **Časť J:** "Prístup k systémom a zdrojom Kupujúceho a ich využívanie"
- **Časť K:** "Odborní pracovníci a bezpečnosť"

Plnenie	Príslušné časti
softvér	A, B, C, D, E, F
Hardware	A, B, C, D, E, F
XaaS / Cloudové služby	A, B, C, D, E, F, G, H, I
odborné služby	A, B, C, J, K

Tabuľka A: Aplikovateľnosť častí ISA

NEDODRŽANIE TEJTO ISA

Ak Dodávateľ v rámci svojho Plnenia zistí akúkoľvek nezhodu s bezpečnostnými opatreniami uvedenými v tejto ISA, potom Dodávateľ Kupujúcemu bezodkladne predloží analýzu situácie a plán pre zaistenie nápravy. Ak bude plán pre zaistenie nápravy Kupujúcim schválený, bude Dodávateľom implementovaný bez akýchkoľvek nákladov pre Kupujúceho a Dodávateľ poskytne dôkaz o účinnosti plánu pre zaistenie nápravy.

Ak nedodržanie požiadaviek pretrváva po dobu viac ako 30 dní, ak nebude v konkrétnom prípade dohodnutá iná lehota a/alebo plán pre zaistenie nápravy nebude schválený Dodávateľom alebo taký plán nezaistí nápravu, bude taký stav automaticky považovaný zapodstatné porušenie zmluvy.

A DODRŽIAVANIE ZMLUVY A NORIEM (ODPORÚČANÝCH TECHNICKÝCH ŠTANDARDOV)

A.1 Hodnotenie bezpečnosti Plnenia

Na žiadosť Kupujúceho poskytne Dodávateľ Kupujúcemu do 10 pracovných dní všetky informácie potrebné pre zhodnotenie bezpečnosti Plnenia, ako sú správy o skúškach / auditoch bezpečnosti, kontroly zraniteľnosti, či analýzy robustnosti kódu.

A.2 Bezpečnostné politiky

Dodávateľ musí mať zavedenú firemnú politiku bezpečnosti informácií, ktoré svojím obsahom zodpovedá norme ISO/IEC 27001 alebo inému podobnému štandardu uznávanému v danom odvetví.

Ak je Dodávateľ certifikovaný, musí Kupujúcemu predložiť svoju bezpečnostnú certifikáciu a priebežne ho informovať o obnovení alebo odstránení svojich certifikátov.

Ak bol Dodávateľ Kupujúcim vybraný na základe určitej certifikácie (napr. ISO / IEC 27001), potom je Dodávateľ povinný takúto certifikáciu udržiavať po celú dobu plnenia svojich zmluvných záväzkov.

A.3 audit

Kupujúci je oprávnený vykonávať audity u Dodávateľa s cieľom overiť dodržiavanie bezpečnostných požiadaviek Kupujúceho definovaných v Zmluve.

A.4 tretie osoby

V prípade, že Dodávateľ pri poskytovaní Plnenia Kupujúcemu využíva tretie osoby, je Dodávateľ povinný zabezpečiť, aby tieto tretie osoby spĺňali bezpečnostné opatrenia dohodnuté v zmluve.

A ORGANIZACE BEZPEČNOSTI

A.1 Struktura

Na žádost Kupujícího je Dodavatel povinen poskytnout informace o organizaci své bezpečnosti.

A.2 Kontaktní místo

Dodavatel jmenuje kontaktní osobu pro bezpečnostní otázky 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.

A.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).

A.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; a
- bude implementován silný autentizační systém (např. dvoufaktorová autentizace).

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

B. ORGANIZÁCIA BEZPEČNOSTI

B.1 Štruktúra

Na žiadosť Kupujúceho je Dodávateľ povinný poskytnúť informácie o organizácii svojej bezpečnosti.

B.2 Kontaktné miesto

Dodávateľ menuje kontaktnú osobu pre bezpečnostné otázky a kontaktnú osobu z radov vyššieho vedenia alebo key account manažéra pre riešenie záležitostí eskalovaných z nižšej úrovne. Kontaktné osoby budú zabezpečené pre každé plnenie a ich zmeny je nutné okamžite oznámiť Kupujúcemu.

B.3 Kontroly bezpečnosti

Raz ročne, na žiadosť jednej alebo oboch Zmluvných strán, usporiadajú Dodávateľ a Kupujúci stretnutie, ktorého cieľom bude vykonať kontrolu bezpečnostných otázok (napr. vývoj a plánované aktivity, ktoré môžu mať vplyv na bezpečnosť).

Každá Zmluvná strana môže požiadať o mimoriadne stretnutie v záležitostiach týkajúcich sa bezpečnosti, pričom druhá Zmluvná strana je povinná túto požiadavku akceptovať v prípadoch, keď situácia vyžaduje spoločnú analýzu alebo okamžité rozhodnutie (napríklad v prípade vážneho incidentu alebo veľkého nárastu hrozieb).

B.4 Bezpečnostné opatrenia pre dáta Kupujúceho

Dodávateľ je povinný zaviesť nasledujúce opatrenia vzťahujúce sa na dáta, ktoré Kupujúci označí za dôverné a:

- všetky uložené a prenášané dáta musia byť zašifrované; a
- bude implementovaný silný autentizačný systém (napr. dvojfaktorová autentizácie).

V prípade nutnosti výmeny zašifrovaných informácií sa zmluvné strany vopred dohodnú na spôsobe ich výmeny.

C RIEŠENIE INCIDENTOV

C.1 Odhaľovanie

Dodávateľ bude mať zavedené opatrenia na detekciu bezpečnostných incidentov, ktoré majú vplyv na Kupujúceho, a ku ktorým dôjde v prostredí Dodávateľa. Medzi bezpečnostné incidenty patria okrem iného strata, zmena, vyzradenie alebo neoprávnený prístup k dátam či informáciám Kupujúceho a ďalej neoprávnené zverejnenie proprietárneho zdrojového kódu.

C.2 Oznamovanie

Dodávateľ akýkoľvek taký bezpečnostný incident Kupujúcemu bezodkladne oznámi.

V prípadoch, keď dôjde k zisteniu akéhokoľvek narušenia a / alebo zneužitia dát alebo informácií Kupujúceho, je Dodávateľ povinný Kupujúceho informovať v súlade s príslušnými právnymi predpismi, najneskôr však do 24 hodín.

Podrobnosti o bezpečnostných incidentoch budú Dodávateľom uchované najmenej do ďalšej bezpečnostnej kontroly vykonávanej Zmluvnými stranami.

C.3 Vyriešenie

Dodávateľ vynaloží všetko úsilie na to, aby bezpečnostné incidenty ihneď vyriešil a bude Kupujúceho informovať o postupe a vyriešenie incidentu.

C.4 Pozastavenie prístupu Dodávateľa k systémom Kupujúceho

POZNÁMKA: Tento odsek C.4 sa nevzťahuje na Software, Plnenie v oblasti Hardwaru a na XaaS / Cloudové služby.

V prípade bezpečnostného incidentu týkajúceho sa Odborných služieb môže Kupujúci pozastaviť prístup Dodávateľa k systémom Kupujúceho do doby, než bude incident vyriešený.

C.5 Pozastavenie prístupu Kupujúceho k Xaas / cloudovým službám

POZNÁMKA: Tento odsek C.5 sa nevzťahuje na Software, Plnenie v oblasti Hardwar u a na Odborné služby.

V prípade bezpečnostného incidentu týkajúceho sa XaaS / cloudových služieb (napr. prienik do systému, incidenty zahŕňajúce malware) môže Kupujúci pozastaviť svoj prístup k uvedenej Službe do doby, než bude incident vyriešený.

V prípade, keď Kupujúci nebude schopný prístup pozastaviť, Kupujúci výslovne požiada Dodávateľa o pozastavenie všetkých prístupov Kupujúceho až do doby vyriešenia incidentu. Dodávateľ takej požiadavke bezodkladne vyhovie.

C.6 Správa o bezpečnosti pre XaaS / Cloudové služby a Odborné služby

POZNÁMKA: Tento odsek C.6 sa nevzťahuje na Plnenie v oblasti Softwar u a Hardwaru.

Kupujúci môže od Dodávateľa požadovať predloženie správy o bezpečnosti týkajúce sa XaaS / cloudových služieb a/alebo Odborných služieb, a to najviac dvakrát ročne. Táto správa o bezpečnosti musí okrem iného obsahovať tieto informácie:

- počet bezpečnostných incidentov zistených za posledných 12 mesiacov, a to oddelene pre vnútorné a vonkajšie príčiny, ak je toto rozdelenie relevantné; a
- podrobnosti o bezpečnostných incidentoch v danom období (čas ich odhalenia, povaha a dopad, vyriešenie, doba obnovy služieb, čas uzavretia, čas nutný na vyriešenie problému).

D ŠIFROVANIE A AUTENTIZÁCIA

D.1 Zmena autentizačných údajov a šifrovacích kľúčov Kupujúcim

Všetky autentizačné údaje a šifrovacie kľúče (napr. certifikáty, páry kľúčov, symetrické kľúče, heslá) v Plnení v oblasti Softwaru a Hardwaru bude Kupujúci môcť zmeniť a budú chránené pomocou najmodernejších (state-of- the- art) technológií. U autentizačných údajov a šifrovacích kľúčov, ktoré Kupujúci nemôže zmeniť, predloží Dodávateľ Kupujúcemu zoznam takýchto údajov vrátane informácií o ich účele. V prípade XaaS / cloudových služieb sa táto požiadavka vzťahuje len na autentizačný údaje využívané Kupujúcim pre ochranu jeho dát.

D.2 Sila šifrovacích algoritmov a kľúčov

Dodávateľ implementuje len štandardizované šifrovacie algoritmy odporúčanej verejnoprávnymi bezpečnostnými autoritami (napr. BSI, Anssi a NIST) v čase uzavretia alebo predĺženia zmluvy.

E BEZPEČNOSŤ NÁVRHU

E.1 Zvýšenie odolnosti

Dodávateľ pri systémoch uplatní štandardné postupy pre zvyšovanie odolnosti (hardening). Tieto postupy zahŕňajú obmedzenia protokolov pre prístup, odstránenie alebo deaktiváciu nepotrebného softwaru, sieťových portov a služieb, odstránenie nepotrebných súborov, užívateľských účtov, obmedzenie povolenia k súborom, správu záplat a protokolovanie.

Dodávateľ poskytne Plnenie (vrátane súčastí a služieb tretích osôb), ktoré bude štandardne (by default) bezpečne nakonfigurované v súlade s najmodernejšími (state-of-the-art) postupmi pre konfiguráciu bezpečnosti (ako sú uvedené napríklad na stránkach https: //www.cisecurity. org /).

Bez ohľadu na vyššie uvedené platí, že Dodávateľ poskytne Kupujúcemu všetky potrebné informácie pre bezpečnú konfiguráciu a využitie Plnenia a zabezpečia, aby takéto informácie boli po celý čas platnosti Zmluvy vždy aktuálne.

Okrem toho je Dodávateľ povinný zabezpečiť, aby Plnenie neobsahovalo žiadne tzv. Zadné vrátka (Back Doors).

E.2 Testovanie softwaru vzhľadom na bezpečnostné chyby

Dodávateľ je povinný vykonať testy Plnenia s cieľom zabezpečiť, že Plnenie nebude k dátumu odovzdania obsahovať žiadne nebezpečné softvérové chyby uvedené v "CWE / SANS Top 25" (http://cwe.mitre.org) a/alebo v "OWASP TOP 10" (http: / /www.owasp.org)(napr. odolnosť voči neočakávaným vstupom, ako je SQL Injection, predvídateľnosť správania v prípadoch preťaženia).

E.3 Dodatočné opatrenia

Na žiadosť Kupujúceho sa môžu Zmluvné strany navzájom dohodnúť na dodatočných bezpečnostných opatreniach, ktoré musí Plnenie spĺňať.

Tieto dodatočné opatrenia môžu byť uvedené v dokumente nazvanom "Vyhlásenie o zhode v oblasti bezpečnosti" (Security Statement of Compliance) a môžu byť obsiahnuté v Zmluve a / alebo v NPA.

F OPRAVY ZRANITELNOSTÍ SOFTWARU

F.1 Odhaľovanie

Dodávateľ zaistí prijatie takých opatrení, ktoré umožnia nepretržité monitorovanie externých zdrojov bezpečnostných informácií (ako sú kooperačné bezpečnostné testy, externý výskum v oblasti bezpečnosti, open source a objavy tretích osôb ...) a bude sledovať Zraniteľnosti, ktoré by mohli mať vplyv na Plnenie (vrátane súčastí tretích osôb).

F.2 CVE Štandard

V prípade potreby bude každej Zraniteľnosti zistené Dodávateľom priradený jedinečný identifikátor CVE spojený so skóre CVSS (verzia 2 alebo vyššia). Akákoľvek alternatíva musí byť písomne schválená Kupujúcim.

F.3 Oznámenie

Dodávateľ bezodkladne poskytne Kupujúcemu informácie o každej Zraniteľnosti (so skóre CVSS vyšším alebo rovným 7,0), a to vrátane Zero-Day, s dopadom na Plnenie a informácie o prípadných dôsledkoch (napr. prípadných CVE, skóre CVSS, dotknutých komponentov alebo služieb).

F.4 Zmluva o úrovni služieb v súvislosti s opravou Zraniteľnosti

Pre každú Zraniteľnosť, ktorá má vplyv na Plnenie, je Dodávateľ povinný:

- poskytnúť Kupujúcemu Dočasnú opravu a Oficiálnu opravu v súlade s nasledujúcou tabuľkou.

základné CVSS skóre v2	**Maximálna lehota na poskytnutie Dočasnej opravy**	**Maximálna lehota na poskytnutie Oficiálnej opravy**
7,0-10,0	7 (sedem) kalendárnych dní	30 (tridsať) kalendárnych dní
0-6,9	neuplatňuje sa	6 (šesť) mesiacov

Meranie tejto lehoty začína v okamihu zistenia Zraniteľnosti - okrem zraniteľnosti súvisiacich so súčasťami od Tretích osôb, kde lehota začína plynúť okamihom, kedy je dostupná oprava.

F.5 Údržba bezpečnosti súčastí Tretích osôb

Dodávateľ zabezpečí, aby súčasti Plnenia poskytnuté tretími osobami, ktoré boli použité v rámci Plnenia na základe Zmluvy mali zaistenú údržbu z hľadiska bezpečnosti po celú dobu údržby alebo Služby zazmluvnenej Kupujúcim.

F.6 Bezpečnostné Nedostatky

Dodávateľ súhlasí s tým, že pre každú Zraniteľnosť ovplyvňujúcu Plnenie, ktorú Kupujúci v priebehu zmluvnej doby údržby a / alebo záručnej doby zistí, je Kupujúci oprávnený zadať Požiadavku na údržbu (maintenance ticket) so žiadosťou o jej odstránenie. Okrem odseku F.4 je Dodávateľ povinný rešpektovať podmienky údržby a odstrániť Nedostatok, ktorý so Zraniteľnosťou súvisí.

F.7 Výnimky

Dodávateľ vynaloží komerčne primerané úsilie na to, aby Kupujúcemu s odstraňovaním zraniteľnosti pomohol:

- v situáciách vyžadujúcich rýchlejšiu reakciu, než je uvedené v tabuľke vyššie (napríklad pri zverejnení Zraniteľnosti Plnenia používaného Kupujúcim prostredníctvom médií); a
- v technickom prostredí nevyhnutnom pre prevádzku Plnenia (napr. v operačnom systéme v prípade softvérového Plnenie).

F.8 Náhrady škody / Pokuty za odstránenie zraniteľností

Okrem opravných postupov, ako aj nárokov v prípade podstatného porušenie, ako je uvedené v odseku "Nedodržanie tejto ISA" vyššie, môže Kupujúci voči Dodávateľovi uplatniť náhradu škody a zmluvnej pokuty v súlade s odsekmi "Náhrada škody" a "Zmluvné pokuty" Zmluvy, ako aj v súlade s nasledujúcim článkom:

V prípade Zraniteľností je Kupujúci oprávnený uplatniť nasledujúce zmluvné pokuty:

Ak Dodávateľ neposkytne Oficiálne opravu Zraniteľnosti sa skóre CVSS vyšším ako 7, ako je uvedené v tabuľke v časti F.4 "Zmluva o úrovni služieb v súvislosti s opravou Zraniteľnosti", vypočíta sa zmluvná pokuta nasledovne:

A = V x N / 300

A: výška pokuty

V: hodnota príslušného Plnenia

N: počet kalendárnych dní, o ktoré bol termín poskytnutia Oficiálne opravy prekročený

Pokuty uvedené v tomto odseku F.8 sú splatné do 30 kalendárnych dní od dátumu doručenia písomnej výzvy na úhradu pokuty. Vznikom nároku na zaplatenie pokuty, jej vyúčtovaním alebo zaplatením nie je dotknutý nárok Kupujúceho na náhradu celkovej ujmy (škody) vzniknutej z rovnakého titulu, a to v plnej výške. Pokuta môže byť Kupujúcim započítaná proti akejkoľvek sume splatnej Kupujúcim Dodávateľovi na základe zmluvy.

F.9 Údržba súvisiace s bezpečnosťou

V priebehu zmluvnej doby údržby a / alebo záručnej doby je Dodávateľ povinný poskytovať Plnenie v oblasti Softwaru a Hardwaru a budúce verzie so všetkými bezpečnostnými záplatami (patch). Tie môžu byť buď nainštalované, alebo poskytované súčasne vo forme samostatného balíka.

V priebehu životného cyklu Plnenia je Dodávateľ povinný poskytovať Kupujúcemu bezpečnostné záplaty v čase a v podobe, v akej budú vydané, a to s rešpektovaním termínov na Opravy zraniteľností definovaných v odseku F.4.

Dodávateľ je povinný poskytnúť Kupujúcemu informácie o zraniteľnosti (napr. CVE, skóre CVSS), ktoré boli záplatami odstránené.

G DÁTA KUPUJÚCEHO V XAAS / CLOUDOVÝCH SLUŽBÁCH

G.1 Obmedzenie používania dát Kupujúceho

Dodávateľ bude dáta Kupujúceho prenášať, spracúvať, vytvárať a / alebo ukladať v XaaS / Cloudové službe iba za účelom poskytovania uvedenej Služby.

G.2 Oddelenie dát Kupujúceho

Dodávateľ bude dbať na oddelenie dát Kupujúceho od dát iných zákazníkov Dodávateľa.

G.3 Dôverné dáta Kupujúceho

Všetky dáta, ktoré budú Kupujúcim klasifikované ako dôverné, budú Dodávateľom pre prenos a uloženie zašifrované.

G.4 Šifrovací mechanizmus Dodávateľa

V prípade, že Kupujúci využíva na ochranu svojich dát šifrovací mechanizmus poskytnutý Dodávateľom, je Dodávateľ povinný zabezpečiť, aby:

- také dáta boli v priebehu uloženia a prenosu zašifrovaná; a
- pre prístup k takýmto dátam bola využívaná silná autentizácia (napr. dvojfaktorová autentizácie).

G.5 Zaznamenávanie (logovanie) prístupu k dátam Kupujúceho a ich použitie

Dodávateľ zaistí:

- zaznamenávanie (logovanie) prístupu k dátam Kupujúceho a ich použitie v rámci XaaS / Cloudové služby, a to vrátane prístupov svojich vlastných zamestnancov a akýchkoľvek poverených tretích osôb; a
- uchovanie takých záznamov (logov) na obdobie dohodnuté v NPA a / alebo Objednávke vrátane súvisiacich dokumentov (napr. v Zmluve o zachovaní mlčanlivosti alebo Zmluve o spracovaní údajov), alebo štandardne po dobu 6 mesiacov.

Výpisy z uchovaných záznamov (logov) budú na požiadanie poskytnuté Kupujúcemu.

G.6 Vrátenie dát Kupujúcemu

Po skončení zmluvy alebo platnosti NPA a / alebo Objednávky vráti Dodávateľ Kupujúcemu všetky dáta Kupujúceho umiestnená v XaaS / Cloudovéj službe, a to vo formáte a po dobu, na ktorých sa s Kupujúcim vopred dohodne.

V súlade s ustanoveniami odseku D. 2 bude pre vrátenie dát Kupujúcim u použité výhradne šifrované pripojenie, ak nedá Kupujúci písomný súhlas s výnimkou z tohto pravidla.

Na konci lehoty na vrátenie dát Dodávateľ zlikviduje všetky prostredia Kupujúceho nachádzajúce sa v XaaS / Cloudovej službe, a to spôsobom, ktorý zaručí, že k žiadnym dátam Kupujúceho nebude naďalej umožnený prístup a dáta nebude možné načítať.

Dodávateľ poskytne Kupujúcemu osvedčenie o takomto zničení.

H RIADENIE PRÍSTUPU K XAAS / CLOUDOVÝM SLUŽBÁM

H.1 Fyzická bezpečnosť

Dodávateľ je povinný zabezpečiť priestory so zodpovedajúcou úrovňou fyzickej bezpečnosti ako pre produkčnú cloudovú infraštruktúru, tak pre lokality pre vzdialené činnosti.

Opatrenia budú spĺňať aspoň nasledujúce požiadavky:

- fyzický prístup vyžaduje oprávnenia a je monitorovaný;
- každý musí byť pri pohybe v priestoroch viditeľne označený oficiálnou identifikáciou;
- návštevy sa musia zapísať do knihy návštev a musia byť pri pohybe v priestoroch sprevádzané a / alebo sledované; a
- držanie kľúčov / prístupových kariet a možnosti prístupu do lokalít sú monitorované. Pracovníci, ktorí ukončia pracovný pomer u Dodávateľa, musia kľúče / karty vrátiť.

H.2 Riadenie prístupu k systému a správa hesiel

Dodávateľ zaistí riadenie prístupov do systémov pre poskytovanie Služieb, pričom prístup bude obmedzený len na oprávnených pracovníkov.

Dodávateľ bude pre súčasti infraštruktúry a systémov pre správu cloudu, ktoré budú slúžiť pre servisné prostredie Dodávateľa, dôsledne uplatňovať politiku hesiel. Dodávateľ zabezpečí ochranu hesiel prostredníctvom bezpečných mechanizmov, ako je napríklad špeciálny nástroj pre ukladanie hesiel (digital vault).

Dodávateľ zavedie systematické riadenie prístupu a jeho evidenciu s cieľom zabezpečiť, aby prístup k systémom mali iba akreditovaní pracovníci prevádzky a podpory. Systematické riadenie prístupu bude zahŕňať autentizáciu, autorizáciu, schválenie vstupu, jeho poskytovanie a odoberanie pre zamestnancov a akýchkoľvek ďalších Dodávateľom definovaných "používateľov".

H.3 Kontrola prístupových práv

Účty pre zamestnancov Dodávateľa v sieti a v operačných systémoch budú pravidelne kontrolované tak, aby sa zabezpečila primeranú úroveň prístupových oprávnení pre príslušných zamestnancov.

V prípade, že niektorý zamestnanec Dodávateľa zmluvný projekt opustí, prijme Dodávateľ rýchle opatrenia, aby ukončil sieťový, telefonický a fyzický prístup takýchto bývalých zamestnancov.

H.4 Bezpečnostné rozhrania (Gateway)

Dodávateľ bude pre riadenie prístupu medzi Internetom a Službami poskytovanými Dodávateľom používať bezpečnostné rozhranie (napr. Brány firewall, routery, servery proxy, reverzné servery proxy) ktoré umožnia iba autorizovanú prevádzku.

Bezpečnostné rozhranie riadené Dodávateľom bude nasadené tak, aby zaisťovali kontrolu paketov, a budú u nich nastavené bezpečnostné pravidlá pre filtrovanie paketov na základe protokolu, portu, zdrojovej a cieľovej IP adresy (podľa potreby), aby bolo možné identifikovať oprávnené zdroje, ciele a typy prevádzky .

H.5 Opatrenia proti malwaru

Dodávateľ bude využívať softvér na ochranu proti malware, ktorý bude slúžiť na kontrolu ukladaných súborov. Definícia malware bude aktualizovaná prinajmenšom raz denne.

H.6 Šifrovanie a vzdialený prístup k XaaS / cloudovým službám

Pre prístup Kupujúceho ku XaaS / Cloudovéj službe a pre jej využívanie musí byť použité výhradne šifrované pripojenie, ak nedá Kupujúci písomný súhlas s výnimkou z tohto pravidla.

Dodávateľ zabezpečí, aby tretie osoby konajúce v mene Dodávateľa a využívajúce vzdialený prístup k dátam Kupujúceho spracovávaným a / alebo uloženým v XaaS / Cloudové službe využívali iba autentizované a šifrované pripojenie.

Vo všetkých prípadoch musí byť pre pripojenie k Xaas / cloudovým službám podporované najnovšie dostupné prehliadače.

I PREVÁDZKA XAAS / CLOUDOVÝCH SLUŽIEB

I.1 Penetračné testy

Dodávateľ bude vykonávať hodnotenie bezpečnosti XaaS / Cloudovéj služby prostredníctvom penetračných testov, a to najmenej raz ročne. Správa z hodnotenia a plán zmierňovanie následkov takých testov budú poskytnuté Kupujúcemu.

Bez ohľadu na vyššie uvedené platí, že Dodávateľ umožní Kupujúcemu vykonávanie penetračných testov na svojej produkčnej platforme.

I.2 Produkčné dáta a prostredie

Dodávateľ nebude pre testovanie využívať produkčné dáta.

Dodávateľ oddelí vývojové, testovacie a produkčné prostredie (siete, dáta, aplikácie atď.).

I.3 Plán obnovy po havárii (Disaster recovery plan)

Dodávateľ vytvorí a bude udržiavať plán obnovy po havárii a zaistí, aby tento plán bol v pravidelných intervaloch testovaný.

Zálohy budú Dodávateľom pri likvidácii bezpečne zmazané.

I.4 Údržba súvisiaca s bezpečnosťou

V prípade akýchkoľvek bezpečnostných záplat (patchov), ktoré Dodávateľ chce nasadiť na Xaas / Cloudové služby, je Dodávateľ povinný danú bezpečnostnú záplatu nasadiť a otestovať v testovacom prostredí. Až po úspešnom dokončení testov v testovacom prostredí môže Dodávateľ záplatu nasadiť v produkčnom prostredí.

I.5 Služby Tretích osôb

Dodávateľ je oprávnený pri poskytovaní Plnenia využívať služby tretej osoby (napr. služby dátového centra), len po predchádzajúcom písomnom schválení Kupujúcim.

J PRÍSTUP K SYSTÉMOM A ZDROJOM KUPUJÚCEHO A ICH VYUŽITIE

Tento odsek sa uplatňuje len v prípadoch, kedy Kupujúci poskytne Dodávateľovi na účely plnenia Zmluvy prístup a umožní mu použitie systémov Kupujúceho.

J.1 Fyzický prístup

Ak Kupujúci poskytne prístup k vybaveniu a/alebo samotné vybavenie pre pripojenie, ktoré je/bude umiestnené v priestoroch Dodávateľa, Dodávateľ zabezpečí, aby:

- sa v technickom priestore, kde sa takéto zariadenie nachádza, uplatnilo riadenie fyzického prístupu; a
- fyzický prístup k takému zariadenia bol obmedzený len na tie osoby, ktoré prístup k takémuto zariadenia potrebujú na účely plnenia Zmluvy a sú Dodávateľom riadne oprávnené.

J.2 Systémy Kupujúceho

Dodávateľ pre ním riadené osoby zabezpečí:

- prístup k systémom Kupujúceho a ich používanie výhradne za účelom poskytovania Plnenia;
- aby prístup a prenosy dát neboli využívané pre vykonanie útoku (napr. na prenos dát, kontroly malware);
- dodržiavanie spôsobov prístupu a pravidiel definovaných Kupujúcim a vopred poskytnutých Dodávateľovi (napr. bude rešpektovať sieťové adresy pridelené Kupujúcim, bude rešpektovať doby odozvy Kupujúceho pre Zdroje riadenie Kupujúceho ...);
- aby každá osoba konajúca za Dodávateľa, ktorá potrebuje používať systémy Kupujúceho, bola Dodávateľom riadne autorizovaná a aby jej identifikačné údaje boli poskytnuté Kupujúcemu; a
- aby k systémom Kupujúceho boli pripojené iba riadne autorizované Zdroje Dodávateľa.

J.3 Systémy a aplikácie Kupujúceho

Ak Kupujúci poskytne Dodávateľovi účty, je Dodávateľ povinný:

- bezodkladne Kupujúceho informovať v prípade, keď daný užívateľský účet nie je naďalej vyžadovaný; a
- zabezpečiť, aby účty poskytnuté pre serverovú komunikáciu boli používané výhradne na tento účel.

J.4 Riadenie Zdrojov Kupujúceho

Ak Kupujúci poskytne Dodávateľovi fyzické zdroje (softvér, hardvér, počítače, USB pamäti, identifikačnú kartu, tablet, smart telefón, prístupové alebo prepojovacie zariadenia ...), je Dodávateľ povinný takéto Zdroje evidovať. Po ukončení zmluvy je Dodávateľ povinný vrátiť zdroje Kupujúceho, ktoré bude mať v tom čase vo svojom držaní.

K ODBORNOSŤ PRACOVNÍKOV A BEZPEČNOSŤ

K.1 Školenie a vzdelávanie (Awareness)

Dodávateľ je povinný zabezpečiť, aby jeho zamestnanci a akékoľvek tretie osoby poverené poskytovaním Plnenia:

- disponovali zodpovedajúcimi schopnosťami v oblasti bezpečnosti (napr. aby boli schopní riešiť bezpečnostné incidenty); a
- boli oboznámení s obsahom a implementáciou príslušných bezpečnostných pravidiel.

K.2 Špecifické bezpečnostné pravidlá Kupujúceho

Ak Kupujúci určí osobitné bezpečnostné pravidlá poskytovania Odborných služieb, je Dodávateľ povinný zabezpečiť, aby jeho zamestnanci a poverené tretie osoby boli pred začatím akýchkoľvek činností o takýchto pravidlách informované.

K.3 Subdodávky

Ak Dodávateľ využíva k plneniu Zmluvy uzatvorenej s Kupujúcim subdodávateľa, musí ich výslovne označiť ako subdodávateľa a zaistiť, že bude z ich strany vždy vynakladá rovnaká riadna starostlivosť.

K.4 Práca s citlivým Plnením

Na žiadosť Kupujúceho sa Dodávateľ zaväzuje využívať k práci s citlivým Plnením, než bude nasadené v Sieti Kupujúceho, a ďalej k údržbe citlivého Plnenia počas celej prevádzkovej fázy iba takých pracovníkov, ktorí prešli bezpečnostnou previerkou, tj. boli preverení príslušnými štátnymi orgánmi.

DEFINÍCIE A SKRATKY

Zmluva	znamená akúkoľvek zmluvu uzavretú medzi Kupujúcim a Dodávateľom, a ktorá odkazuje na túto ISA.
aktíva	zahŕňa primárne a podporné aktíva, ako sú definované v ISO / IEC 27005.
Zadné vrátka ("Back Doors")	znamená funkciu alebo vadu Plnenia, ktorá umožňuje skrytý neoprávnený prístup k dátam.
CVE	znamená bežné zraniteľnosti a riziká definované na: http://cve.mitre.org/index.html.
CVSS	znamená Common Vulnerability Scoring System (Systém hodnotenia bežných zraniteľností), ako je definovaný na: http://www.first.org/cvss/ .
Nedostatok	znamená akúkoľvek odchýlku aktuálnej kvality Plnenia od zmluvou zamýšľanej kvality, napr. neplnenie, nezhodu Plnenia s jeho príslušnou špecifikáciou alebo neschopnosť Plnenia fungovať v súlade s príslušnou dokumentáciou.
plnenie	znamená všetky zariadenia, produkty a / alebo služby objednané podľa hlavnej zmluvy, vrátane všetkých hlavných alebo dodatočných záväzkov.
bezpečnosť informácií	znamená - v súlade s ISO / IEC 27001 a ISO / IEC 27005 - bezpečnosť v rozsahu spracovania informácií a činností (primárnych aktív) spoliehajúcich na technické (vrátane, okrem iného, IT, priestor, zariadení a sietí) a netechnické zdroje (vrátane, okrem iného, podporných aktív, ako napr. personálu, partnerov, organizácií, postupov, obchodných podmienok).
internet vecí	znamená akákoľvek pripojené zariadenia alebo vybavenie určené pre internet vecí.
NPA	znamená zmluvu uzavretú s akoukoľvek sesterskou spoločnosťou Kupujúceho na základe Rámcovej zmluvy, ktorá môže byť prípadne uzavretá. NPA zodpovedá pojmom "Realizačná zmluva", "Zmluva pre konkrétny projekt" a "Zmluva o projekte": každé ustanovenie využívajúce pojem "NPA" sa vzťahuje aj na tieto druhy zmlúv.
Oficiálna oprava	znamená, že je dostupné kompletné riešenie Dodávateľa k oprave Zraniteľnosti formou oficiálnej (riadne) záplaty (patch) alebo upgrade.
objednávka	znamená nákupnú objednávku vystavenú Kupujúcim. "Objednávka" zodpovedá pojmu "Nákupná objednávka" uvádzanému v zmluvách uzatvorených Kupujícím a jeho sesterskými spoločnosťami. Každé ustanovenie používajúce pojem "Objednávka" sa obdobne vzťahuje na "Nákupnú objednávku".
kupujúci	znamená Kupujúceho, ako aj jeho sesterskú spoločnosť , ktorá je zmluvnou stranou NPA alebo Objednávky. "Kupujúci" zodpovedá pojmu "Objednávateľ" uvádzanému v zmluvách uzatvorených Kupujúcim a je ho sesterskými spoločnosťami. Každé ustanovenia vzťahujúce sa na Kupujúceho v tejto ISA sa tiež analogicky vzťahuje na "Objednávateľa".
sieť Kupujúceho	znamená sieť spravovanú Kupujúcim a všetku súvisiacu infraštruktúru pre prístup k Sieti Kupujúceho nevyhnutnú pre zabezpečenie komunikácie medzi zdrojmi jednotlivých strán.
zdroje Kupujúceho	znamená hardvér, softvér, služby patriace Kupujúcemu a používané za účelom poskytovania Plnenia.
výsledný Software	znamená akýkoľvek softvér, ktorý: (i) primárne vychádza z požiadavky Kupujúceho a/alebo Špecifikácie poskytnutej Kupujúcim alebo výlučne pre Kupujúceho a / alebo ktorý sa týmito požiadavkami riadi a / alebo (ii) bol vyvinutý alebo implementovaný Dodávateľom na základe tejto zmluvy (a / alebo akýchkoľvek jej neskorších dodatkov) a / alebo akoukoľvek NPA a / alebo Objednávkou, a ktorý nie je určený k behu na pozadí; môže alebo nemusí byť chránený právami duševného vlastníctva, a ďalej akékoľvek produkty alebo procesy z neho vyplývajúce.
Vyhlásenie o zhode	znamená prílohu zmluvy s podrobnými technickými požiadavkami na bezpečnosť Plnenia.

Špecifikácia diela (Statement of Work - Sow)	znamená dokument definujúci špecifické činnosti, plnenie a časový harmonogram Dodávateľa v súvislosti s poskytovaním Plnenie a / alebo Služieb Kupujúcemu v rámci daného projektu.
zdroje Dodávateľa	znamená hardvér, softvér patriaci a / alebo v zodpovednosti Dodávateľa, ktoré sú využívané na účely poskytovania Plnenie.
dočasná oprava	znamená prípad, keď je dostupná oficiálna (riadna) , avšak dočasná oprava Zraniteľnosti, vrátane, okrem iného, dočasnej opravy, nástrojov alebo dočasných riešení (workaround).
zraniteľnosť	znamená slabinu znižujúce dostupnosť, integritu alebo dôvernosť informácií.
XaaS	znamená čokoľvek, čo je užívateľom poskytované ako služba, vrátane SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) či podobné.
Nultý deň (Zero-Day)	znamená doteraz neurčenú zraniteľnosť, ktorú môžu hackeri využiť pre nepriaznivé ovplyvnenie Plnenie. Táto zraniteľnosť známa pod názvami "zero-day" (alebo "zero-hour" alebo "0-day" alebo "day zero " alebo "zraniteľnosť nultého dňa") , pretože nebola do jej využitia verejne ohlásená či oznámená, čo ponecháva Dodávateľovi nula dní, počas ktorých musí vytvoriť záplatu alebo odporučiť dočasné riešenie (workaround) pre zmiernenie jej vplyvu.

Príloha č. 1

BCM Požiadavky

1) Na zabezpečenie ochrany podnikania ST/TMCZ je Dodávateľ povinný zaviesť a udržiavať účinný systém kontinuity podnikania v zhode s ISO 22301. Tento systém musí zahŕňať aj pravidelné testovanie plánov kontinuity činností pre uistenie, že v prípade mimoriadne alebo krízové situácie a bezprostredne po nej bude Dodávateľ schopný pokračovať v plnení záväzkov voči ST/TMCZ.
2) Dodávateľ zabezpečí dostatočnú mieru odolnosti a obnoviteľnosti predmetu dodávky tak, aby bolo zaručené dosiahnutie cieľov doby zotavenia (RTO), ako sú ustanovené v dohode o úrovni poskytovaných služieb (SLA) pre každú poskytovanú službu.
3) Počas tzv. Prechodnej fázy kontraktu preukáže Dodávateľ svoju schopnosť obnovy všetkých dodávaných služieb vytvorením príslušnej dokumentácie, ktorá bude následne testovaná z pohľadu presnosti a úplnosti.
4) Dodávateľ zavedie a bude udržiavať systém riadenia rizík (vrátane identifikácie rizík, ich kontroly a procesu akceptácie) pre dodávané služby a relevantné platformy.
5) Dodávateľ oznámi bezodkladne ST/TMCZ zistené alebo potenciálne riziká relevantné pre dodávanú službu.
6) Dodávateľ poskytne ST/TMCZ zoznam známych rizík, vzťahujúcich sa ku všetkým aktívam relevantným pre dodávanú službu. Dodávateľ vykonáva analýzu dopadov (BIA) pre poskytované služby a platformy a identifikuje vplyvy a zraniteľnosti podľa metodiky dohodnutej s ST/TMCZ.
7) Dodávateľ je zodpovedný za vytváranie, údržbu a testovanie dokumentácie BCM v rozsahu dodávaných služieb a platforiem. ST/TMCZ bude v tejto oblasti s Dodávateľom spolupracovať.
8) Dodávateľ bude vykonávať revízie BCM dokumentácie v pravidelných intervaloch a s každou významnou zmenou, najmenej však jedenkrát ročne. Zmeny budú podliehať schvaľovanie TMSK.
9) Dodávateľ zabezpečí udržiavanie povedomie svojich príslušných zamestnancov o obsahu dokumentácie BCM k predmetu dodávky, preveruje správne pochopenie obsahu dokumentácie a vykonáva pravidelné školenia a aktualizácie.
10) Dodávateľ zaistí dostatok vyškolených zamestnancov v pohotovosti pre prípad riešenia mimoriadnej udalosti.
11) ST/TMCZ overí pripravenosti Dodávateľa splniť záväzky z BCM pomocou pravidelných cvičení.
12) Dodávateľ bude realizovať testovanie zavedených opatrení systému kontinuity podnikania podľa požiadaviek zmluvy minimálne 1x ročne.
13) Dodávateľ bude spolupracovať s ST/TMCZ pri dohodnutých cvičeniach BCM.
14) Dodávateľ bude informovať najmenej jeden mesiac vopred ST/TMCZ, pokiaľ bude pripravovať cvičenia BCM a po ukončení cvičenia odovzdá ST/TMCZ správu o výsledkoch cvičenia.
15) ST/TMCZ si vyhradzuje právo vykonať audit systému kontinuity podnikania u Dodávateľa. ST/TMCZ akceptuje aj audit nezávislej audítorskej autority, ak sa vzťahuje k predmetu dodávky.
16) ST/TMCZ si pre overenie funkčnosti plánov obnovy Dodávateľa vyhradzuje právo zúčastniť sa jeho Disaster Recovery cvičenia.
17) ST/TMCZ si vyhradzuje právo nahliadať do BCM dokumentácie dodávateľa.
18) Dodávateľ bezodkladne oznámi ST/TMCZ identifikačné údaje outsourcigového partnera, ak predmet dodávky, alebo jeho časti budú outsourcované.
19) Dodávateľ bude po svojich kritických dodávateľoch požadovať aspoň rovnakú mieru zaistenie kontinuity činností, ako ST/TMCZ požaduje po ňom.
20) Dodávateľ vykoná bezodkladne (najneskôr však do 3 mesiacov) implementáciu potrebných opatrení, definovaných auditom, alebo vzídených z testov, cvičenie, porúch, analýzy rizík, alebo procesu riadenia zmien, týkajúce sa predmetu dodávky.
21) Dodávateľ poskytne ST/TMCZ informácie a nálezy z auditu ISO 27001 a 22301, najmä zistenia týkajúce schopnosti Dodávateľa poskytovať predmet dodávky.
22) Dodávateľ bezodkladne nahlási ST/TMCZ všetky bezpečnostné incidenty, ktoré spôsobili, alebo môžu spôsobiť výpadok predmetu dodávky.
23) Dodávateľ a ST/TMCZ si dohodnú pravidlá a požiadavky na riešenie incidentov.

Príloha č. 3

Subdodávatelia

Obchodná firma (IČO, adresa, zápis v OR)	Poskytované služby	Zavedený/certifikovaný systém podľa čl. 1.1 Zmluvy
		Áno / Nie