



Korporátne pravidlá informačnej bezpečnosti a ochrany dát

1. Tieto Korporátne pravidlá informačnej bezpečnosti a ochrany dát (ďalej len „Pravidlá“) sa aplikujú na záväzkové vzťahy medzi spoločnosťou Slovak Telekom, a.s. (ďalej len “ST”) a druhou zmluvnou stranou (ďalej len “Dodávateľ”), vznikajúce pri ich podnikateľskej činnosti, zahŕňajúc najmä nákupné objednávky vystavené ST, kúpne zmluvy, zmluvy o dielo a ostatné zmluvy podľa II. hlavy 3. časti zákona č. 513/1991 Zb. Obchodného zákonníka v znení neskorších predpisov, ako aj akékoľvek iné zmluvy uzavreté medzi spoločnosťou ST a Dodávateľom (ďalej len “Zmluva”), ktorých predmetom je najmä dodanie hnuťelných vecí (tovarov), zhotovenie diela a/alebo poskytovanie služieb (ďalej ako „Činnosti“) zo strany Dodávateľa spoločnosti ST (ďalej len “Plnenie”).
2. Dodávateľ sa zaväzuje pri poskytovaní Plnenia podľa Zmluvy dodržiavať požiadavky nasledujúcich medzinárodných štandardov:

Zavedený	Certifikovaný	Systém
Áno	Áno	Systém managementu kvality podľa ISO 9001
Áno	Áno	Systém environmentálneho managementu podľa ISO 14001
Áno	Áno	Systém managementu bezpečnosti informácií podľa ISO 27001
Áno	Áno	Systém riadenia kontinuity podľa ISO 22301
Áno	Áno	Systém manažmentu služieb v informačných technológiách podľa ISO 20000-1
Áno	Áno	Systém riadenia energetickej efektívnosti podľa ISO50 001

3. Dodávateľ sa zaväzuje poskytovať Plnenie podľa Zmluvy a zabezpečovať výkon Činností, ku ktorým sa zaviazal podľa Zmluvy, primárne prostredníctvom svojich zamestnancov. V prípade, že Dodávateľ využije subdodávateľa, musí byť tento subdodávateľ schválený zo strany ST a musí byť uvedený v Prílohe č.3 týchto Pravidiel a/ alebo Zmluve, pokiaľ sa Dodávateľ a ST nedohodli inak. Pokiaľ sa Dodávateľ a ST výslovne nedohodli inak, Dodávateľ nie je oprávnený poveriť výkonom svojich povinností podľa Zmluvy žiadneho subdodávateľa bez predchádzajúceho písomného súhlasu spoločnosti ST.
4. Ak ST udelí Dodávateľovi súhlas s použitím konkrétneho subdodávateľa, je Dodávateľ povinný uzavrieť s týmto subdodávateľom zmluvu, ktorá zabezpečí, aby subdodávateľ vykonával povinnosti podľa Zmluvy za rovnakých podmienok a za rovnakej kvality, ako je medzi ST a Dodávateľom dohodnuté v Zmluve tak, aby bolo zabezpečené dodržanie požiadaviek ST definovaných Zmluvou. Dodávateľ je plne zodpovedný za riadne a včasné plnenie týchto povinností subdodávateľom. Predovšetkým, ale nie výlučne, sa takýto subdodávateľ musí zaviazat' k dodržiavaniu všetkých požiadaviek a povinností Dodávateľa podľa týchto Pravidiel. Osobitne musia byť zmluvne ošetrené so subdodávateľom podmienky pre prístup, práva a povinnosti pre zabezpečenie ochrany všetkých technických, obchodných alebo iných informácií (ďalej len „Dôverné informácie“), s ktorými sa Dodávateľ oboznámil počas trvania Zmluvy, bez ohľadu na to či sú tieto Dôverné informácie označené ako dôverné. Povinnosť zabezpečiť dôvernosť pretrváva aj po skončení Zmluvy.
5. V prípade, že Dodávateľ má zavedený alebo certifikovaný systém, ktorý je uvedený v bode 1 týchto Pravidiel, potom je povinný predložiť ST 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 vyššie uvedenými medzinárodnými štandardmi, ako aj Zmluvou. V prípade, že Dodávateľ poskytuje plnenie podľa Zmluvy pomocou a/alebo prostredníctvom schválených subdodávateľov, ktorí majú niektorý z týchto systémov zavedený či certifikovaný, zabezpečí Dodávateľ súhlas s vykonaním auditov aj u týchto subdodávateľov, a to za účelom preverenia zhody s predmetnými medzinárodnými štandardmi.



6. 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 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 plnením podľa Zmluvy. V prípade, že Dodávateľ poskytuje plnenie podľa Zmluvy za pomoci a/alebo prostredníctvom schválených subdodávateľov, ktorí nemajú niektorý zo systémov zavedený či certifikovaný, zabezpečí Dodávateľ súhlas s vykonaním auditu aj u týchto subdodávateľov, a to za účelom preverenia zhody so Zmluvou.
7. 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 všetky informácie (napr. správy z auditov), ktoré sa týkajú schopnosti Dodávateľa poskytovať plnenie podľa Zmluvy. Ak implementácia nápravných opatrení bude trvať po dobu dlhšiu než 30 dní, ak nebude v konkrétnom prípade dohodnutá iná lehota a/alebo plán pre zabezpečenie nápravy nebude schválený Dodávateľom alebo takýto plán nezabezpečí nápravu a ani Dodávateľ neoznámí výhrady k navrhnutým nápravným opatreniam v určenej lehote, bude taký stav automaticky považovaný za podstatné porušenie Zmluvy, pričom ST je v takom prípade oprávnený odstúpiť od Zmluvy. V prípade, ak požiadavku na vykonanie nápravného opatrenia vzniesť príslušný štátny orgán v zmysle platnej právnej úpravy alebo je vykonanie nápravného opatrenia nevyhnutné z dôvodu plnenia zákonných povinností ST alebo potreby riešenia bezpečnostného incidentu, Dodávateľ je povinný poskytnúť požadovanú súčinnosť v lehote určenej ST a jej včasné neposkytnutie sa považuje za podstatné porušenie Zmluvy s právom odstúpiť od Zmluvy. .
8. Dodávateľ musí mať zavedený systém riadenia kontinuity činností, aby bol schopný ST 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 súčinnosť pri príprave a realizácii plánov kontinuity činností alebo obnovy po havárii v ST. Dodávateľ je povinný pri poskytovaní Plnenia podľa Zmluvy dodržiavať požiadavky na riadenie kontinuity činností uvedené v Prílohe č. 2 týchto Pravidiel, za predpokladu že plnenie podľa Zmluvy bude vyhodnotené z analýzy obchodných dopadov (BIA) ako kritické a / alebo existuje zákonný dôvod pre riadenie Dodávateľa v oblasti riadenia kontinuity činností (BCM).
9. Dodávateľ je povinný nakladať s odpadmi, ktorých je pôvodcom alebo vlastníkom v súvislosti s plnením podľa Zmluvy, v súlade so všeobecne záväznými právnymi predpismi, najmä tými upravujúcimi oblasť odpadov.
10. Zamestnanci, personál, poverené osoby a subdodávateľia Dodávateľa (ďalej len „Poverené osoby“) vstupujúci do priestorov alebo objektov ST a vykonávajúci tam Činnosti podľa Zmluvy, sú povinné zoznámiť sa s dokumentáciou bezpečnosti a ochrany zdravia pri práci, ochrany pred požiarmi a požiarno-technickými zariadeniami umiestnených v priestoroch príslušného objektu ST.
11. 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.
12. Dodávateľ sa zaväzuje pri plnení Zmluvy dodržiavať všetky všeobecne záväzné právne predpisy ako aj ostatné aplikovateľné predpisy (napr. STN) na zabezpečenie bezpečnosti a ochrany zdravia pri práci.



13. 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. Pre umožnenie vstupu osôb a/alebo vjazd dopravných prostriedkov do priestorov a objektov ST bude Dodávateľovi vydané potrebné povolenia vydané príslušným oddelením ST. Dodávateľ si o povolenie požiada prostredníctvom kontaktnej osoby podľa bodu 22 a 23 týchto Pravidiel.
14. Za oboznámenie Poverených osôb Dodávateľa s relevantnými internými predpismi ST, odovzdanie Prístupových prostriedkov určených pre Poverené osoby zodpovedá zodpovedná osoba ST.
15. Dodávateľ berie na vedomie, že ním Poverené osoby sa podrobia kontrole vykonávanej v súlade s internými predpismi ST (napr. fyzická kontrola osôb a dopravných prostriedkov, technická kontrola zariadenia) pri vstupe do priestorov ST. Poverené osoby, ktoré vykonávajú činnosť v priestoroch ST sú povinné sa pred vstupom do týchto priestorov identifikovať (napr. zamestnaneckým preukazom, preukazom totožnosti, občianskym preukazom, cestovným pasom).
16. V prípade, že Dodávateľovi budú odovzdané Prístupové prostriedky do priestorov či objektov ST, je Dodávateľ povinný dodržiavať interné predpisy ST týkajúce sa Prístupových prostriedkov. Dodávateľ nesmie vyhotoviť duplikát alebo kópiu z prevzatého Prístupového prostriedku.
17. Dodávateľ a ním Poverené osoby sú oprávnené pri výkone plnenia podľa tejto Zmluvy zdržiavať sa a pohybovať sa v priestoroch a objektoch ST len v čase potrebnom pre uskutočnenie dohodnutých Činností a Služieb, a to len v priestoroch a objektoch, ktoré sú pre tieto Činnosti určené.
18. Dodávateľ a ST berú na vedomie a súhlasia s tým, že všetky informácie obsiahnuté v Zmluve ako aj v nadväzujúcich zmluvách a informácie vymieňané medzi ST a Dodávateľom v súvislosti s poskytovaním Plnenia podľa Zmluvy, budú považované za dôverné a chránené v rozsahu podmienok dohodnutých v Zmluve a/alebo dohode o zachovávaní dôvernosti uzavretej medzi ST, a Dodávateľom (ďalej len "NDA") a/alebo inej súvisiacej osobitnej dohode upravujúcej podmienky ochrany informácií (napr. pre oblasť ochrany osobných údajov, kybernetickú bezpečnosť a pod). Pokiaľ nie je v Zmluve dohodnuté inak, v prípade rozporov medzi ustanoveniami NDA a Zmluvy, majú vždy prednosť ustanovenia Zmluvy a ustanovenia osobitných dôhod pred Zmluvou.
19. Dodávateľ sa zaväzuje vytvoriť, používať a udržiavať primerané technické, organizačné a personálne bezpečnostné opatrenia na zabezpečenie dôvernosti, dostupnosti a integrity Dôverných informácií, ktoré mu boli alebo budú poskytnuté alebo sprístupnené zo strany ST alebo jej zmluvných partnerov. Tieto opatrenia musia byť dostatočné, aby sa zabránilo náhodnému alebo neoprávnenému zničeniu, strate, zámene, sprístupneniu údajov alebo akýmkoľvek neoprávneným formám využívania Dôverných informácií. Dodávateľ je povinný udržiavať tieto opatrenia vo funkčnom stave počas celého obdobia využívania Dôverných informácií.
20. Pri poskytovaní Plnenia podľa Zmluvy je Dodávateľ zodpovedný za to, že Plnenie bude dodané bez vád, s náležitou starostlivosťou a v súlade s podmienkami uvedenými v Zmluve ako aj v Prílohe č. 1 týchto Pravidiel.
21. Dodávateľ prehlasuje, že Plnenie podľa Zmluvy bude jeho menom dodané iba prostredníctvom zamestnancov, ktorí sú vo vzťahu k charakteru Plnenia bezúhonní a spĺňajúci potrebné kvalifikačné predpoklady a že je schopný toto na vyžiadanie ST aj preukázať. Táto povinnosť platí obdobne pre subdodávateľov, ktorí sa menom Dodávateľa budú podieľať na poskytovaní Plnenia.
22. Dodávateľ je povinný zabezpečiť ochranu dôvernosti a integritu všetkých prístupových prostriedkov (prístupové ID, heslá, tokeny čipové karty, vstupné karty, kľúče a pod.) do



elektronických systémov a priestorov ST (ďalej len „Prístupové prostriedky“), ktoré sú Dodávateľovi sprístupnené na základe Zmluvy a nesmie ich sprístupniť tretím osobám. Dodávateľ je povinný bezodkladne oznámiť ST stratu, krádež, zneužitie alebo zničenie Prístupového prostriedku v súlade s čl. 27 týchto Pravidiel.

23. Dodávateľ sa zaväzuje, že poučí svoje Poverené osoby, že sú povinné najmä:
 - a) pre vstup a výstup do a z priestorov ST 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 ST;
 - 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;
 - g) bezodkladne oznámiť ST stratu, krádež, poškodenie, zneužitie Prístupového prostriedku, ako aj o zmenách údajov obsiahnutých na Prístupovom prostriedku;
 - h) na vyzvanie zamestnanca ST sa preukázať Prístupovým prostriedkom;
 - i) neumožniť vstup do objektu ST žiadnej osobe;
 - j) po ukončení zmluvnej činnosti vrátiť Prístupový prostriedok, ako aj všetky ďalšie veci patriace ST.
24. Dodávateľ a všetky osoby podieľajúce sa na poskytovaní Plnenia podľa Zmluvy v jeho mene, sú povinní podriaďovať sa a rešpektovať zavedené bezpečnostné opatrenia ST a bezpečnostné pokyny ST a nie sú oprávnení vykonávať žiadne činnosti, ktoré by mohli tieto opatrenia narušiť alebo poškodiť.
25. Dodávateľ je vždy povinný informovať ST, pokiaľ niektorá z jeho Poverených osôb ukončí svoj pracovnoprávny (dodávateľský) vzťah s Dodávateľom a zároveň je povinný vrátiť všetky poskytnuté Prístupové prostriedky, ktoré ST tejto osobe poskytol. V prípade straty Prístupových prostriedkov je Dodávateľ povinný nahradiť ST vzniknutú škodu.
26. Dôverné údaje s veľkým objemom budú medzi ST a Dodávateľom vymieňané výlučne spôsobom, ktorý zaručí dôvernosť a integritu prenášaných údajov (napr. prenosom pomocou SFTP protokolu súborami, ktoré majú stanovený dohodnutý typ a formát).
27. ST a Dodávateľ zriadia spoločný bod kontaktu pre riešenie všetkých problémov, vzájomné poskytovanie informácií, spoluprácu v oblasti bezpečnosti informácií a ochrany dát a určia kontaktné osoby za obe strany. V prípade zmeny tejto osoby sa Dodávateľ zaväzuje bezodkladne určiť novú kontaktnú osobu a oznámiť ST jej kontaktné informácie.
28. Dodávateľ je povinný bezodkladne ohlásiť ST akúkoľvek neštandardnú situáciu, podozrivé udalosti, bezpečnostné incidenty a stratu Prístupového prostriedku, a to prostredníctvom nasledujúcich kontaktov: email: security@telekom.sk, tel. : +421 800 100 166.
29. Dodávateľ je povinný v rámci spolupráce s ST vynaložiť maximálne úsilie, aby zabránil pokračovaniu bezpečnostného incidentu, predišiel ďalším bezpečnostným incidentom, zabezpečil a obnovil všetky opatrenia potrebné na ochranu dát a informácií ST.
30. Pokiaľ bude pri poskytovaní Plnenia podľa tejto Zmluvy dochádzať k vykonávaniu Činností priamo súvisiacich s dostupnosťou, dôvernosťou a integritou prevádzky 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 (ďalej len „ZoKB“), 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, resp. § 22 ods. 4 ZoKB.

31. Pokiaľ sa Dodávateľ a ST v Zmluve alebo inej osobitnej dohode výlovne nedohodnú inak, Dodávateľ nebude mať prístup v rámci poskytovaní Plnenia podľa Zmluvy prístup k
 - a) akýmkoľvek osobným údajom zákazníkov a zamestnancov ST v zmysle nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
 - b) akýmkoľvek údajom, ktoré tvoria predmet telekomunikačného tajomstva v zmysle zákona č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov.

32. Dodávateľ je povinný zabezpečiť, aby počítačový program (zdrojový a strojový kód), ktorý dodá ST v rámci Plnenia, obsahoval len kód vyvinutý v súlade s požiadavkami Zmluvy, požiadavkami Prílohy č. 1 týchto Pravidiel a v súlade s aplikovateľnými štandardmi podľa bodu 2 týchto Pravidiel. Dodávateľ sa najmä zaväzuje, že kód nebude obsahovať žiadne zlomyseľné a/alebo škodlivé prvky či bezpečnostné slabiny umožňujúce narušenie bezpečnosti Plnenia, a že nebude obsahovať žiadny malvér (tak ako je definovaný nižšie). Prístup ku kódu bude Dodávateľ riadiť, obmedzovať na nevyhnutný okruh poverených osôb a chrániť proti neoprávnenej manipulácii.

33. Dodávateľ je povinný zabezpečiť ochranu pred škodlivými kódmi a malvérmi. Malvérom 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 hardvéru, 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.

34. Pokiaľ sa ST a Dodávateľ nedohodnú inak, Dodávateľ sa zaväzuje zabezpečiť:
 - a) že pre vývojové a testovacie účely použije samostatne vyvinuté testovacie anonymizované dáta,
 - b) ochranu dôvernosti, dostupnosti a integrity testovacích dát,
 - c) samostatné vývojové a testovacie prostredie oddelené od živého prevádzkového systému,
 - d) bezodkladnú bezpečnú preukázateľnú likvidáciu testovacích dát po skončení potreby ich použitia,
 - e) pred odovzdaním Plnenia podľa Zmluvy do prevádzky akceptačné testy, ktorých súčasťou sú aj bezpečnostné testy.

35. V prípade porušenia ktorejkoľvek povinností vyplývajúcej z týchto Pravidiel je ST oprávnená požadovať od Dodávateľa zaplatenie zmluvnej pokuty vo výške 100.000,- EUR (slovami: jedno sto tisíc eur), a to za každý jednotlivý prípad. Zmluvná pokuta je splatná na základe faktúry vystavenej spoločnosťou ST bez zbytočného odkladu po porušení príslušnej povinnosti, a to do 14 dní od jej vystavenia. Dodávateľ sa zaväzuje, že zmluvnú pokutu zaplatí riadne a včas. Zaplatením zmluvnej pokuty nie je dotknutý nárok na náhradu škody vo výške presahujúcej zmluvnú pokutu.



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 posilnené o dodatočné bezpečnostné opatrenia, ktoré budú zabezpečené Kupujúcim a dohodnuté medzi Zmluvnými stranami v dokumentoch priložených k Zmluve, NPA a/alebo Objednávke, alebo akoukoľvek inou súvisiacou zmluvou, ktorá takéto bezpečnostné opatrenia bude riešiť (napr. zmluva uzatvorená podľa Zákona o kybernetickej bezpečnosti).

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 (štandardný) softvér a / alebo individuálne vytvorený softvér vychádzajúci zo Špecifikácie diela vzájomne dohodnuté medzi Zmluvnými stranami (napr. Výsledný Software);
- **Hardvér** 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/Odborné služby** pre zabezpečenie inštalácie, školenia, integrácie, údržby a / alebo poradenstvo;



- **Plnenia Dodávateľa, na ktoré sa vzťahujú požiadavky Zákona o kybernetickej bezpečnosti** v platnom znení a predstavujú plnenia týkajúce sa prvkov a informačných systémov, ktoré sú prvkom kritickej infraštruktúry Kupujúceho a/alebo ktoré priamo súvisia s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov Kupujúceho ako poskytovateľa základnej služby (ďalej aj „Plnenia týkajúce sa kybernetickej bezpečnosti“).

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 Zraniteľností"
- **Časť G:** "Dáta Kupujúceho v: XaaS / cloudových službách, Plnenia týkajúce sa kybernetickej bezpečnosti"
- **Časť H:** "Riadenie prístupu k: XaaS / cloudovým službám, Plnenia týkajúce sa kybernetickej bezpečnosti "
- **Časť I:** "Prevádzka: XaaS / cloudových služieb, Plnenia týkajúce sa kybernetickej bezpečnosti "
- **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
Hardvér	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
Plnenia týkajúce sa kybernetickej bezpečnosti	A, B, C, D, E, F, G, H, I, J, K

Tabuľka A: Aplikovateľnosť častí ISA

NEDODRŽANIE TEJTO ISA

Ak Dodávateľ v rámci svojho Plnenia zistí akúkoľvek nehodu s bezpečnostnými opatreniami uvedenými v tejto ISA, potom Dodávateľ Kupujúcemu bezodkladne predloží analýzu situácie a plán pre zabezpečenie



nápravy. Ak bude plán pre zabezpečenie nápravy Kupujúcim schválený, bude Dodávateľom implementovaný bez akýchkoľvek nákladov pre Kupujúceho a Dodávateľ poskytne dôkaz o účinnosti plánu pre zabezpečenie nápravy.

Ak nedodržanie požiadaviek pretrváva po dobu viac ako 30 dní, ak nebude v konkrétnom prípade dohodnutá iná lehota a/alebo plán pre zabezpečenie nápravy nebude schválený Dodávateľom alebo taký plán nezaistí nápravu, bude taký stav automaticky považovaný za podstatné porušenie zmluvy, pričom Kupujúci je v takom prípade oprávnený odstúpiť od 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. Pokiaľ Dodávateľ poskytuje Kupujúcemu Plnenia týkajúce sa kybernetickej bezpečnosti, je povinný poskytovať Kupujúcemu všetky potrebné informácie, súčinnosť a spoluprácu.

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 organizačné a technické bezpečnostné opatrenia dohodnuté v Zmluve.

B ORGANIZÁCIA BEZPEČNOSTI

B.1 Štruktúra

Na žiadosť Kupujúceho je Dodávateľ povinný poskytnúť informácie o organizácii svojej bezpečnosti, vrátane systému riadenia kybernetickej bezpečnosti pokiaľ sa táto povinnosť Dodávateľa týka.

B.2 Kontaktné miesto

Dodávateľ menuje kontaktnú osobu pre bezpečnostné otázky, oznamovanie incidentov alebo iných udalostí 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 zavedie a dodržiava bezpečnostné opatrenia podľa stupňa klasifikácie dát Kupujúceho. Dodávateľ je povinný zaviesť nasledujúce opatrenia vzťahujúce sa na dáta Kupujúceho:

- všetky uložené a prenášané dáta musia byť zašifrované;
- k spracúvaným dátam budú mať prístup len oprávnené osoby; a
- bude implementovaný silný autentizačný systém (napr. dvojfaktorová autentizácia).

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

Dodávateľ je povinný spracúvať dáta Kupujúceho prostredníctvom zavedeného systému riadenia identít a prístupových práv. Taktiež je dodávateľ povinný riadiť všetky privilegované prístupy a výnimky z procesu riadenia identít a prístupových práv.

C RIEŠENIE INCIDENTOV

C.1 Odhaľovanie

Dodávateľ bude mať zavedené opatrenia na detekciu a riadenie 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 a taktiež kybernetické bezpečnostné incidenty podľa Zákona o kybernetickej bezpečnosti.

C.2 Oznamovanie

Dodávateľ akýkoľvek bezpečnostný incident vrátane všetkých skutočností majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti bezodkladne oznámi Kupujúcemu.

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, bezodkladne.

Podrobnosti o bezpečnostných incidentoch budú Dodávateľom uchované v súlade s príslušnými právnymi predpismi, 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 vyriešení incidentu vrátane prijatia nápravných opatrení.

C.4 Pozastavenie prístupu Dodávateľa k systémom Kupujúceho

POZNÁMKA: Tento odsek C.4 sa nevzťahuje na XaaS / Cloudové služby.

V prípade bezpečnostného incidentu 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 Softvér, Plnenie v oblasti Hardvéru, Odborné služby a Plnenia týkajúce sa kybernetickej bezpečnosti.

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

Kupujúci môže od Dodávateľa požadovať predloženie správy o bezpečnosti týkajúce sa poskytovaných Plnení a to najviac dvakrát ročne; tým nie je dotknuté právo Kupujúceho požadovať potrebné informácie priebežne kedykoľvek, ak je to potrebné v súvislosti s plnením jeho zákonných povinností. 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).
- Všetky informácie, ktoré bude Kupujúci požadovať v súvislosti s plnením jeho zákonných povinností a požiadaviek, najmä v súvislosti s platnou legislatívou v oblasti kybernetickej bezpečnosti a ochrany súkromia.

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 Softvéru, Hardvéru a Plnení týkajúcich sa kybernetickej bezpečnosti 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 autentizačné 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 softvéru, 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 SOFTWARE

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 Plnenia).

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 nárok na náhradu škody a zmluvnej pokuty v súlade s ustanoveniami Zmluvy upravujúcimi "Náhradu škody" a "Zmluvné pokuty", ako aj v súlade s nasledujúcim článkom:

V prípade Zraniteľností je Kupujúci oprávnený uplatniť nasledujúce zmluvné pokuty:

Ak Dodávateľ neposkytne Oficiálnu opravu Zraniteľnosti so skóre CVSS minimálnym a 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:

$$A = V \times N / 300$$

A: výška pokuty

V: hodnota príslušného Plnenia

N: počet kalendárnych dní, o ktoré bol termín poskytnutia Oficiálnej 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 Softvéru a Hardvéru 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, PLNENIA TÝKAJÚCE SA KYBERNETICKEJ BEZPEČNOSTI

G.1 Obmedzenie používania dát Kupujúceho

Dodávateľ bude dáta Kupujúceho prenášať, spracúvať, vytvárať a / alebo ukladať v XaaS / Cloudovej 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 zašifrované; a
- pre prístup k takýmto dátam bola využívaná silná autentizácia (napr. dvojfaktorová autentizácia).

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

Dodávateľ zabezpečí:

- zaznamenávanie (logovanie) prístupu k dátam Kupujúceho a ich použitie, 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 dôvernosti alebo Zmluve o spracovaní osobných údajov), alebo inak 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, 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 Kupujúcemu 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 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, PLNENIA TÝKAJÚCE SA KYBERNETICKEJ BEZPEČNOSTI

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 malvéru, ktorý bude slúžiť na kontrolu ukladaných súborov. Definícia malvéru bude aktualizovaná prinajmenšom raz denne.

H.6 Šifrovanie a vzdialený prístup

Pre prístup Kupujúceho ku XaaS / Cloudovej 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 / Cloudovej 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, PLNENIA TÝKAJÚCE SA KYBERNETICKEJ BEZPEČNOSTI

I.1 Penetračné testy

Dodávateľ bude vykonávať hodnotenie bezpečnosti poskytovaných Plnení prostredníctvom penetračných testov, a to najmenej raz ročne. Správa z hodnotenia a plán zmiernenie 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 zaistiť, 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 pri poskytovaní Plnenia, 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 zariadeniu bol obmedzený len na tie osoby, ktoré prístup k takému zariadeniu 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 prenosi dát boli zabezpečené šifrovacími prostriedkami a neboli využívané pre vykonanie útoku a iné nevhodné aktivity (napr. na prenos dát, kontroly malvéru);
- dodržiavanie spôsobov prístupu a pravidiel definovaných Kupujúcim (vrátane pravidiel dobrej praxe) a vopred poskytnutých Dodávateľovi (napr. bude rešpektovať sieťové adresy pridelené Kupujúcim, bude rešpektovať doby odozvy Kupujúceho pre Zdroje riadenie Kupujúceho ...);
- v prípade využívania vzdialeného prístupu k systémom Kupujúceho, dodržiavanie povinnosti Dodávateľa dodržiavať pravidlá, spôsoby a postupy špecifikované Kupujúcim;
- aby každá osoba konajúca za Dodávateľa, ktorá potrebuje používať systémy Kupujúceho, bola Dodávateľom riadne autorizovaná a aby jej identifikačné údaje boli poskytnuté Kupujúcemu a zoznam konajúcich (oprávnených) osôb bol priebežne udržiavaný a aktualizovaný 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 a prevádzka informačno-komunikačných technológií Kupujúceho

Ak Dodávateľ poskytuje Plnenia týkajúce kybernetickej bezpečnosti Kupujúceho, je dodávateľ povinný:

- dodržiavať pravidlá prepájania systémov Kupujúceho a prenosu elektronických informácií;
- riadiť bezpečnosť sietí a zmien infraštruktúry podľa pravidiel a pokynov Kupujúceho;
- uplatniť riadenie kapacity systémov a služieb podľa pravidiel a pokynov Kupujúceho;
- využívať riadené kryptografické opatrenia; a
- mať implementovaný systém riadenia kontinuity procesov a činností a zabezpečiť zosúladenie so systémom riadenia kontinuity Kupujúceho.

J.5 Riadenie Aktív Kupujúceho

Ak Kupujúci poskytne Dodávateľovi Aktíva Kupujúceho je Dodávateľ povinný takéto Aktíva Kupujúceho evidovať a riadiť prístup k nim za uplatnenia náležitej klasifikácie takýchto Aktív. Obdobný prístup Dodávateľ uplatňuje aj v prípade spracúvania osobných údajov sprístupnených Kupujúcim.

Po ukončení zmluvy je Dodávateľ povinný vrátiť Aktíva Kupujúceho, ktoré bude mať v tom čase vo svojom držaní. Taktiež je Dodávateľ povinný po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky



potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie prevádzkovej základnej služby na Kupujúceho, ktorý je v pozícii prevádzkovateľa základnej služby; tento záväzok Dodávateľa ostáva v platnosti aj po ukončení zmluvného vzťahu najmenej po dobu päť rokov po ukončení zmluvného vzťahu, ak nebude dohodnuté inak.

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);
- boli oboznámení s obsahom a implementáciou príslušných bezpečnostných pravidiel a všetky aktivity vykonávali podľa týchto pravidiel; a
- dodržiavali mlčanlivosť o všetkých skutočnostiach a informáciách Kupujúceho a podpísali prehlásenie o zachovávaní mlčanlivosti.

K.2 Špecifické bezpečnostné pravidlá Kupujúceho

Ak Kupujúci určí osobitné bezpečnostné pravidlá poskytovania Odborných služieb a Plnení týkajúcich sa kybernetickej bezpečnosti, 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 plánuje využiť k plneniu Zmluvy uzatvorenej s Kupujúcim subdodávateľa, môže tak konať iba po predchádzajúcom súhlase Kupujúceho, musí ich výslovne označiť ako subdodávateľa a zabezpečiť a zmluvne zaviazat', že bude z ich strany vždy vynakladaná rovnaká riadna starostlivosť. Takéto vynakladanie riadnej starostlivosti platí pre všetky subdodávateľské vzťahy vrátane akvizície, vývoja a údržby systémov a aplikácií.

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 preverkou, tj. Boli preverení príslušnými štátnymi orgánmi.

DEFINÍCIE A SKRATKY

Zmluva	znamená akúkoľvek zmluvu uzavretú medzi Kupujúcim a Dodávateľom, 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, nezohodu Plnenia s jeho príslušnou špecifikáciou alebo neschopnosť Plnenia fungovať v súlade s príslušnou dokumentáciou.
Plnenie	znamená všetky zariadenia, produkty a / alebo služby a činnosti objednané podľa 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 aktíva (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 kompletne 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 Kupujúcim a jeho sesterskými spoločnosťami. Každé ustanovenie používajúce pojem „Objednávka“ sa obdobne vzťahuje na „Nákupnú objednávku“.
Kupujúci	znamená Slovak Telekom, a.s., 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 ustanovenie 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.
Aktíva Kupujúceho	Znamená najmä informácie, procesy, 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 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 Plnenia. 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.
Zákon o kybernetickej bezpečnosti	Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v platnom znení, vrátane súvisiacich vykonávacích predpisov, a prípadne iný právny predpis, ktorý ho v budúcnosti nahradí.



Príloha č. 2 - BCM Požiadavky

- 1) Na zabezpečenie ochrany podnikania ST 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.
- 2) Dodávateľ zabezpečí dostatočnú mieru odolnosti a obnoviteľnosti predmetu Plnenia tak, aby bolo zaručené dosiahnutie cieľov doby zotavenia (RTO), ako sú ustanovené v dohode o úrovni poskytovaných služieb (SLA) pre každé poskytované Plnenie.
- 3) Počas tzv. Prechodnej fázy kontraktu preukáže Dodávateľ svoju schopnosť obnovy všetkých poskytovaných Plnení 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 Plnenia a relevantné platformy.
- 5) Dodávateľ oznámi bezodkladne ST zistené alebo potenciálne riziká relevantné pre poskytované Plnenie.
- 6) Dodávateľ poskytne ST zoznam známych rizík, vzťahujúcich sa ku všetkým aktívam relevantným pre poskytované Plnenie. Dodávateľ vykonáva analýzu dopadov (BIA) pre poskytované Plnenie a platformy a identifikuje vplyvy a zraniteľnosti podľa metodiky dohodnutej s ST.
- 7) Dodávateľ je zodpovedný za vytváranie, údržbu a testovanie dokumentácie BCM v rozsahu dodávaných Plnení a platformiem. ST 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 schvaľovaniu zo strany ST.
- 9) Dodávateľ zabezpečí udržiavanie povedomie svojich príslušných zamestnancov o obsahu dokumentácie BCM k predmetu Plnenia, 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 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 pri dohodnutých cvičeniach BCM.
- 14) Dodávateľ bude informovať najmenej jeden mesiac vopred ST, pokiaľ bude pripravovať cvičenia BCM a po ukončení cvičenia odovzdá ST správu o výsledkoch cvičenia.
- 15) ST si vyhradzuje právo vykonať audit systému kontinuity podnikania u Dodávateľa. ST akceptuje aj audit nezávislej auditorskej authority, ak sa vzťahuje k predmetu Plnenia.
- 16) ST/TMCZ si pre overenie funkčnosti plánov obnovy Dodávateľa vyhradzuje právo zúčastniť sa jeho Disaster Recovery cvičenia.
- 17) ST si vyhradzuje právo nahliadať do BCM dokumentácie dodávateľa.
- 18) Dodávateľ bezodkladne oznámi ST identifikačné údaje outsourcingového partnera, ak predmet Plnenia, alebo jeho časti budú outsourcované.
- 19) Dodávateľ bude po svojich kritických dodávateľoch požadovať aspoň rovnakú mieru zabezpečenia kontinuity činností, ako ST požaduje po ňom.
- 20) Dodávateľ vykoná bezodkladne (najneskôr však do 3 mesiacov) implementáciu potrebných opatrení, definovaných auditom, alebo vziđených z testov, cvičenie, porúch, analýzy rizík, alebo procesu riadenia zmien, týkajúce sa predmetu Plnenia.
- 21) Dodávateľ poskytne ST informácie a nálezy z auditu ISO 27001 a 22301, najmä zistenia týkajúce schopnosti Dodávateľa poskytovať predmet Plnenia.
- 22) Dodávateľ bezodkladne nahlási ST všetky bezpečnostné incidenty, ktoré spôsobili, alebo môžu spôsobiť výpadok predmetu Plnenia.
- 23) Dodávateľ a ST si dohodnú pravidlá a požiadavky na riešenie incidentov.



Príloha č. 3 - Schválení Subdodávateľa

Spoločnosť (obchodné meno, IČO, sídlo, zápis v OR)	Poskytované Plnenia	Zavedený/certifikovaný systém podľa bodu 2 Pravidiel
		Áno / Nie