Informačná Bezpečnosť

- ďalej uvádzaná ako „ISA“ -

VŠEOBECNÉ ZÁSADY

Tento dokument Informačná Bezpečnosť (ISA) ustanovuje opatrenia pre informačnú bezpečnosť. Ak platí pre predmet dodávky špecifikovaný v Zmluve, dodávateľ musí považovať tieto opatrenia za minimálny bezpečnostný štandard a musia platiť počas trvania Zmluvy, bez ohľadu na to či je predmet dodávky zabezpečovaný na základe Zmluvy alebo prostredníctvom jeho subdodávateľov.

Tieto opatrenia pokrývajú rôzne aspekty informačnej bezpečnosti a niektoré sa uplatňujú v závislosti od povahy predmetu dodávky, ktorej sa týka Zmluva.

VŠEOBECNÉ UPLATNENIE ISA

Dodávateľ musí splniť požiadavky ISA pre všetky zložky predmetu dodávky definované v nasledujúcom texte:

- **Softvér** označuje hotový softvér predajcu alebo špeciálny softvér na objednávku vyplývajúci z výkazu prác/technickej špecifikácie vzájomne dohodnutej stranami (napr. softvérový výsledok);
- **Hardvér** vrátane vloženého softvéru/firmvéru (napr. zariadenie koncového používateľa a zariadenia pre Internet vecí, IT vybavenie, atď.);
- **Služby XaaS/Cloud** (napr. softvér ako služba); a
- **Odborné služby** na vykonávanie inštalácie, školení, integrácie, údržby alebo poradenstva.

VŠEOBECNÉ UPLATNENIE ŠPECIFICKÝCH ČASTÍ TÝKAJÚCICH SA PREDMETU DODÁVKY

Nasledujúce časti platia pre akýkoľvek typ predmetu dodávky dodávateľa:

- **Časť A:** „Dodržiavanie zmlúv a noriem“
- **Časť B:** „Organizácia bezpečnosti“
- **Časť C:** „Riadenie incidentov“

Nasledujúce časti sa uplatňujú podľa povahy predmetu dodávky definovanej v tabuľke A:

- **Časť D:** „Kryptografia a overovanie“
- **Časť E:** „Bezpečnosť v dizajne (Security by design)“
- **Časť F:** „Náprava zraniteľnosti softvéru"
- **Časť G:** „Údaje kupujúceho v službách XaaS/Cloud“
- **Časť H:** „Kontrola prístupu v službách XaaS/Cloud“
- **Časť I:** „Operácie v službách XaaS/Cloud“
- **Časť J:** „Prístup a používanie systémov a zdrojov kupujúceho"
- **Časť K:** „Odbornosť a bezpečnosť"

Predmet dodávky	Uplatňované časti
Softvér	A, B, C, D, E, F
Hardvér	A,B, C, D, E, F
Služby XaaS/Cloud	A, B,C, D, E, F, G, H, I
Odborné služby	A, B, C, J, K

Tabuľka A: Uplatňovanie častí ISA

A DODRŽIAVANIE ZMLÚV A NORIEM

A.1 Hodnotenie bezpečnosti predmetu dodávky

Na požiadanie kupujúceho dodávateľ poskytne kupujúcemu do 10 pracovných dní všetky informácie potrebné na posúdenie bezpečnosti predmetu dodávky ako bezpečnostný test/audítorské správy, skeny zraniteľnosti a analýzy robustnosti kódov.

A.2 Bezpečnostné zásady

Dodávateľ musí uplatňovať podnikovú politiku informačnej bezpečnosti podľa normy ISO/IEC 27001 alebo podobnej uznávanej praxe.

Ak je dodávateľ certifikovaný, poskytne kupujúcemu svoj bezpečnostný certifikát a bude ho informovať o obnovení alebo zrušení svojich certifikátov.

Ak si kupujúci vybral dodávateľa na základe certifikácie (napr. ISO/IEC 27001), dodávateľ musí udržiavať takúto certifikáciu počas celého trvania jeho zmluvných povinností.

A.3 Audit

Kupujúci má právo vykonávať audity na kontrolu, či dodávateľ dodržiava bezpečnostné požiadavky kupujúceho a Orange definované v Zmluve.

A.4 Tretie strany

V prípade, že dodávateľ na poskytovanie predmetu dodávky kupujúcemu využíva tretie strany, dodávateľ zabezpečí, aby tieto tretie strany spĺňali bezpečnostné opatrenia dohodnuté v zmluve.

A.5 Nedodržiavanie ISA

V prípade, že sa dodávateľ dozvie o nedodržaní bezpečnostných opatrení v predmete dodávky, bezodkladne poskytne kupujúcemu analýzu situácie a plán nápravy. Ak kupujúci akceptoval plán nápravy, dodávateľ ho zrealizuje bez nákladov pre kupujúceho a dodávateľ poskytne dôkaz o účinnosti plánu nápravy.

Ak nesúlad pretrváva, alebo plán nápravy nie je prijatý alebo zlyhá, automaticky to znamená závažné porušenie zmluvy.

B ORGANIZÁCIA BEZPEČNOSTI

B.1 Štruktúra

Na požiadanie kupujúceho dodávateľ poskytne informácie o svojej organizácii bezpečnosti.

B.2 Kontaktný bod

Dodávateľ vymenuje kontaktnú osobu pre bezpečnosť nasledovne: ……..

B.3 Hodnotenia bezpečnosti

Raz ročne, na žiadosť jednej alebo oboch strán, dodávateľ a kupujúci zorganizujú stretnutie na preskúmanie bezpečnostných aspektov (napr. vývoj a naplánované operácie, ktoré môžu mať vplyv na bezpečnosť).

Každá zmluvná strana môže požiadať o mimoriadne bezpečnostné stretnutie, ktoré druhá strana prijme, ak situácia vyžaduje spoločnú analýzu alebo okamžité rozhodnutie (napríklad väčší incident alebo závažný vývoj hrozby).

B.4 Bezpečnostné opatrenia pre údaje kupujúceho

Dodávateľ zavedie nasledujúce opatrenia pre údaje, ktoré kupujúci klasifikoval ako dôverné:

- pri ukladaní a prenose budú všetky údaje šifrované; a
- bude zavedený silný systém overovania (napr. systém dvojfaktorového overovania).

Strany sa vopred dohodnú na spôsobe výmeny v prípade, že si potrebujú vymeniť šifrované informácie.

C RIADENIE INCIDENTOV

C.1 Odhaľovanie

Dodávateľ musí mať zavedené opatrenia na odhaľovanie bezpečnostných incidentov ovplyvňujúcich kupujúceho a vyskytujúcich sa v prostredí dodávateľa. Bezpečnostné incidenty zahŕňajú, ale nielen, stratu, zmenu, zverejnenie alebo neoprávnený prístup k údajom alebo informáciám kupujúceho alebo nepovolené odhalenie vlastníckeho zdrojového kódu.

C.2 Oznamovanie

Dodávateľ takéto bezpečnostné incidenty okamžite oznámi kupujúcemu.

Ak sa zistí porušenie alebo zneužitie údajov alebo informácií kupujúceho, dodávateľ to oznámi kupujúcemu podľa platných zákonov, ale najneskôr do 24 hodín.

Podrobnosti o bezpečnostných incidentoch si dodávateľ uchová aspoň až do ďalšieho hodnotenia bezpečnosti medzi stranami.

C.3 Vyriešenie

Dodávateľ vynaloží všetko úsilie na okamžité vyriešenie bezpečnostných incidentov a bude informovať kupujúceho o postupe a konci incidentu.

C.4 Pozastavenie prístupu dodávateľa k systému kupujúceho

POZNÁMKA: Tento bod C.4 neplatí pre softvérové, hardvérové časti predmetu dodávky a služby XaaS/Cloud.

V prípade bezpečnostného incidentu týkajúceho sa odborných služieb kupujúci môže až do vyriešenia incidentu pozastaviť prístup dodávateľa k systému kupujúceho.

C.5 Pozastavenie prístupu kupujúceho k službám Xaas/Cloud

POZNÁMKA: Tento bod C.5 neplatí pre softvérové, hardvérové časti predmetu dodávky a odborné služby.

V prípade bezpečnostného incidentu týkajúceho sa služieb XaaS/Cloud (napr. vniknutie do systému, malvérový incident) môže kupujúci pozastaviť jeho prístup k uvedenej službe až do vyriešenia incidentu.

V prípade ak kupujúci nie je schopný pozastaviť prístup, kupujúci výslovne požiada dodávateľa, aby pozastavil všetky prístupy kupujúceho až do vyriešenia incidentu. Dodávateľ okamžite splní takúto žiadosť.

C.6 Správa o bezpečnosti služieb XaaS/Cloud a odborných služieb

POZNÁMKA: Tento bod C.6 neplatí pre softvérové a hardvérové časti predmetu dodávky.

Kupujúci môže požadovať od dodávateľa správu o bezpečnosti týkajúcu sa služieb XaaS/Cloud a odborných služieb najviac dvakrát do roka. Táto správa o bezpečnosti musí zahŕňať, ale nielen, nasledujúce informácie:

- počet bezpečnostných incidentov zistených za posledných 12 mesiacov, zvlášť pre interné a externé príčiny, ak je to relevantné; a
- detaily bezpečnostných incidentov počas toho obdobia (čas odhalenia, povaha a dosah, vyriešenie, doba na obnovu služby, čas uzávierky, čas vyriešenia).

D KRYPTOGRAFIA A OVEROVANIE

D.1 Zmena overovacích údajov a šifrovacích kľúčov kupujúcim

Všetky overovacie údaje a kryptografické kľúče (napr. certifikáty, páry kľúčov symetrické kľúče, heslá) v softvérových a hardvérových častiach predmetu dodávky bude kupujúci meniť a chrániť podľa najnovších technológií. Pokiaľ ide o overovacie údaje a kryptografické kľúče, ktoré kupujúci nemôže meniť, dodávateľ poskytne kupujúcemu zoznam takýchto údajov a ich účel. Pri službách XaaS/Cloud sa táto požiadavka vzťahuje iba na overovacie údaje, ktoré kupujúci používa na ochranu svojich údajov.

D.2 Sila kryptografických algoritmov a kľúčov

Dodávateľ bude zavádzať len štandardizované kryptografické algoritmy odporúčané vládnymi inštitúciami (napríklad BSI, ANSSI a NIST) v čase uzavretia alebo obnovenia zmluvy.

E BEZPEČNOSŤ V DIZAJNE (SECURITY BY DESIGN)

E.1 Posilnenie ochrany (hardening)

Dodávateľ použije štandardizované postupy na posilnenie ochrany systému. To zahŕňa obmedzenie prístupu k protokolu, odstránenie alebo deaktiváciu nepotrebného softvéru, sieťových portov a služieb, odstránenie nepotrebných súborov, používateľských účtov, obmedzenie povolení pre súbor, riadenie opráv a protokolovanie.

Dodávateľ poskytne predmet dodávky (vrátane komponentov a služieb tretích strán) bezpečne nakonfigurovaný štandardne podľa postupov konfigurácie v súlade s najnovšími technológiami (ako napr. https://www.cisecurity.org/) .

Bez ohľadu na vyššie uvedené dodávateľ poskytne kupujúcemu všetky potrebné informácie na bezpečné konfigurovanie a používanie predmetu dodávky a zabezpečí, že takéto informácie budú vždy aktuálne počas trvania zmluvy.

Okrem toho, dodávateľ zabezpečí, aby predmet dodávky neobsahoval žiadne „zadné vrátka“ (Back Doors).

E.2 Zisťovanie bezpečnostných chýb softvéru

Dodávateľ vykoná testy predmetu dodávky, aby sa uistil, že neobsahujú nebezpečné softvérové chyby uvedené v „CWE / SANS Top 25“ (http://cwe.mitre.org) a/alebo „OWASP TOP 10“ (http://www.owasp.org) v čase dodania (napr. odolnosť proti neočakávaným vstupom, ako sú SQL Injection, predvídateľné správanie v situáciách preťaženia, atď.).

E.3 Ďalšie opatrenia

Na požiadanie kupujúceho sa strany môžu vzájomne dohodnúť na doplňujúcich bezpečnostných opatreniach, ktoré musí spĺňať predmet dodávky.

Tieto doplňujúce opatrenia môžu byť zhrnuté v dokumente s názvom „Bezpečnostné vyhlásenie o zhode“ a môžu byť zahrnuté v zmluve alebo v NPA.

F NÁPRAVA ZRANITEĽNOSTI SOFTVÉRU

F.1 Odhaľovanie

Dodávateľ musí mať zavedené opatrenia na nepretržité monitorovanie externých bezpečnostných poradenských zdrojov (napríklad kooperatívne bezpečnostné testy, externé skúmanie bezpečnosti, odhalenia otvoreného zdrojového kódu a odhalenia treťou stranou,...) a sledovať zraniteľnosti, ktoré by mohli ovplyvniť predmet dodávky (vrátane komponentov tretej strany).

F.2 Norma CVE

Ak je to vhodné, každá zistená zraniteľnosť bude mať jedinečný identifikátor CVE spojený so skóre podľa CVSS (v2 alebo vyšší). Iná alternatíva musí byť písomne dohodnutá s kupujúcim.

F.3 Oznámenia

Dodávateľ okamžite poskytne kupujúcemu informácie o každej zraniteľnosti (so skóre podľa CVSS väčším alebo rovnajúcim sa 7.0) vrátane Zero-Day, ktoré ovplyvňujú predmet dodávky, a ich dôsledkoch (napr. CVE, ak existuje, skóre CVSS, dotknuté komponenty alebo služby).

F.4 Dohoda o úrovni poskytovaných služieb na nápravu zraniteľností

Pre každú zraniteľnosť ovplyvňujúcu predmet dodávky dodávateľ:

- vynaloží všetko úsilie, aby poskytol kupujúcemu dočasnú opravu podľa nasledujúcej tabuľky; a
- sprístupní kupujúcemu oficiálnu opravu podľa nasledujúcej tabuľky.

Základ CVSS **Skóre v2**	**Maximálny čas na poskytnutie** **dočasnej opravy**	**Maximálny čas na poskytnutie** **oficiálnej opravy**
7.0-10.0	7 (sedem) kalendárnych dní	30 (tridsať) kalendárnych dní
0-6.9	nehodí sa	6 (šesť) mesiacov;

Čas sa začne odpočítavať od zistenia zraniteľnosti, s výnimkou zraniteľnosti nachádzajúcej sa v komponentoch tretej strany, keď sa počítanie času začne, keď je k dispozícii oprava.

F.5 Udržiavanie bezpečnosti komponentov tretej strany

Dodávateľ zabezpečí, aby počas obdobia údržby alebo služby zmluvne zabezpečenej kupujúcim bola zabezpečovaná bezpečnosť komponentov tretej strany použitých v predmete dodávky.

F.6 Bezpečnostné chyby

Dodávateľ bude akceptovať, že pre každú zraniteľnosť, ktorá ovplyvňuje predmet dodávky a ktorú odhalil kupujúci počas zmluvného obdobia údržby a/alebo záručnej doby, kupujúci môže otvoriť údržbový tiket na jej opravu. Okrem časti F.4 dodávateľ bude rešpektovať aj podmienky údržby na opravu chyby súvisiacej so zraniteľnosťou.

F.7 Výnimky

Dodávateľ musí vynaložiť komerčne primerané úsilie na podporu kupujúceho pri oprave zraniteľností:

- v prípadoch vyžadujúcich rýchlejšiu odozvu ako v tabuľke uvedenej vyššie (napr. zverejnenie zraniteľnosti v predmete dodávky, ktorý používa kupujúci); a
- v technickom prostredí potrebnom na prevádzku predmetu dodávky (napr. operačný systém pre softvérový predmet dodávky).

F.8 Náhrada škody/sankcie za opravy zraniteľnosti

Okrem opravných prostriedkov v dôsledku závažného porušenia, ako je uvedené v časti A.5 „Nedodržiavanie ISA", si kupujúci môže voči dodávateľovi uplatniť sankcie dohodnuté v zmluve a/alebo náhradu škody.

F.9 Údržba súvisiaca s bezpečnosťou

Počas zmluvného obdobia údržby alebo záručnej doby bude dodávateľ poskytovať softvérové a hardvérové časti predmetu dodávky a budúce verzie so všetkými bezpečnostnými záplatami. Tieto verzie sa môžu buď aplikovať alebo budú poskytnuté zároveň ako samostatný balík.

Počas životného cyklu predmetu dodávky dodávateľ poskytne kupujúcemu bezpečnostné záplaty, ako a keď sú vydané, pričom bude dodržiavať čas opravy zraniteľnosti určený v časti F.4.

Dodávateľ poskytne kupujúcemu informácie (napríklad CVE, CVSS skóre) o zraniteľnostiach, ktoré boli opravené v záplatách.

G ÚDAJE KUPUJÚCEHO V SLUŽBÁCH XAAS/CLOUD

G.1 Obmedzenie používania údajov kupujúceho

Dodávateľ bude používať údaje kupujúceho prenášané, spracované, vytvorené alebo uložené v službe XaaS/Cloud iba na poskytovanie uvedenej služby.

G.2 Segregácia údajov kupujúceho

Dodávateľ musí oddeliť údaje kupujúceho od údajov ostatných zákazníkov dodávateľa.

G.3 Dôverné údaje kupujúceho.

Dodávateľ pri prenose a uložení zašifruje všetky údaje, ktoré kupujúci označí ako dôverné.

G.4 Šifrovacie mechanizmy dodávateľa

V prípade, že kupujúci využíva na ochranu údajov kupujúceho mechanizmus šifrovania poskytnutý dodávateľom, dodávateľ zabezpečí, aby:

- takéto údaje boli pri ukladaní a prenose šifrované; a
- sa pre prístup k takýmto údajom používalo silné overovanie (napr. dvojfaktorové overovanie).

G.5 Prihlasovanie sa pre prístup a používanie údajov kupujúceho

Dodávateľ :

- zaznamenáva prístup k údajom a ich používanie v službe XaaS/Cloud, vrátane jeho zamestnancov a akýchkoľvek určených tretích strán; a
- uchováva takéto záznamy po dobu dohodnutú v NPA a/alebo objednávke vrátane súvisiacich dokumentov (napr. zmluva o zachovaní mlčanlivosti alebo zmluvy o spracovaní údajov) alebo štandardne 6 mesiacov.

Na požiadanie budú kupujúcemu poskytnuté výpisy z uchovávaných záznamov.

G.6 Vrátenie údajov kupujúceho

Pri ukončení NPA a/alebo objednávky dodávateľ umožní kupujúcemu získať späť všetky údaje kupujúceho v službe XaaS/Cloud vo formáte a na dobu vzájomne vopred dohodnutú s kupujúcim.

Podľa časti D2 na vrátenie údajov sa pre kupujúceho použijú iba šifrované pripojenia, pokiaľ kupujúci písomne nesúhlasil s výnimkou.

Na konci obdobia vracania údajov dodávateľ zničí všetky prostredia kupujúceho a údaje kupujúceho v službe XaaS/Cloud spôsobom, ktorý je navrhnutý tak, aby sa zabezpečilo, že nemôžu byť prístupné alebo prečítané.

Dodávateľ poskytne kupujúcemu potvrdenie o zničení.

H „KONTROLA PRÍSTUPU V SLUŽBÁCH XAAS/CLOUD“

H.1 Fyzická bezpečnosť

Dodávateľ poskytne fyzicky zabezpečené zariadenie pre výrobnú cloudovú infraštruktúru a miesta na diaľkové operácie.

Riadiace prvky zahŕňajú prinajmenšom:

- fyzický prístup vyžaduje povolenie a je sledovaný;
- každý musí na pracovisku viditeľne nosiť oficiálnu identifikáciu;
- návštevníci musia podpísať záznam návštev a musia byť v priestoroch sprevádzaní a/alebo sledovaní; a
- vlastnenie kľúčov/prístupových kariet a možnosť prístupu na miesta sa monitoruje. Pracovníci, ktorí odchádzajú zo zamestnania u dodávateľa, musia vrátiť kľúče/karty.

H.2 Riadenie systému prístupu a spravovanie hesiel

Dodávateľ musí kontrolovať systémy služby obmedzením prístupu iba pre oprávnených pracovníkov.

Dodávateľ musí na komponentoch infraštruktúry a systémoch riadenia cloudov, ktoré sa používajú na prevádzku prostredia služieb dodávateľa, uplatňovať politiku hesiel. Dodávateľ musí chrániť heslá pomocou bezpečných mechanizmov, ako napríklad digitálny trezor.

Dodávateľ musí zaviesť systém riadenia prístupu a zodpovednosti navrhnutý tak, aby zabezpečil, že k systémom majú prístup len schválení zamestnanci pre jednotlivé operácie a podporu. Riadenie prístupu k systému zahŕňa systém overovania, povolenie, schválenie prístupu, poskytovanie a zrušenie pre zamestnancov a iných „používateľov“ definovaných dodávateľom.

H.3 Prehodnotenie prístupových práv

Pravidelne sa budú prehodnocovať účty zamestnancov dodávateľa v sieti a operačnom systéme, aby boli zabezpečené príslušné úrovne prístupu pre zamestnancov.

V prípade, že zamestnanec dodávateľa odíde zo zmluvného projektu, je dodávateľ povinný prijať okamžité opatrenia na ukončenie prístupu takýchto bývalých zamestnancov do siete, aj telefonického a fyzického prístupu.

H.4 Bezpečnostná brána

Dodávateľ musí používať bezpečnostné brány (napr. firewally, routery, proxy, reverzné proxy) na riadenie prístupu medzi Internetom a službami dodávateľa tým, že povolí iba autorizovanú prevádzku.

Dodávateľ rozmiestni bezpečnostné brány, ktoré bude spravovať, na vykonávanie kontroly paketov s bezpečnostnými zásadami konfigurovanými pre filtrovanie paketov na základe protokolu, portu, zdroja a cieľovej adresy IP, ako je to vhodné, za účelom zistenia overených zdrojov, destinácií a typov prevádzky.

H.5 Kontrola malvéru

Dodávateľ musí používať antimalvérový softvér na skenovanie sťahovaných súborov. Definície malvéru sa aktualizujú minimálne každý deň.

H.6 Šifrovanie a vzdialené pripojenie k službám XaaS / Cloud

Pre prístup kupujúceho k službe XaaS / Cloud a jej používanie musia byť použité iba šifrované spojenia, ak kupujúci písomne neschváli výnimku.

Dodávateľ musí zabezpečiť, aby sa pre tretie strany konajúce v mene dodávateľa, ktoré majú vzdialený prístup k údajom kupujúceho spracovávaným a/alebo ukladaným v službe XaaS / Cloud, používali len overené a šifrované spojenia.

Vo všetkých prípadoch musia byť najnovšie dostupné prehliadače podporované pre pripojenie k službám Xaas / Cloud.

I OPERÁCIE V SLUŽBÁCH XAAS/CLOUD

I.1 Penetračné testy

Dodávateľ posúdi bezpečnosť služby XaaS / Cloud pomocou penetračných testov aspoň raz ročne. Správu a plán zmiernenia dôsledkov z týchto testov musí oznámiť kupujúcemu.

Bez ohľadu na uvedené je dodávateľ povinný umožniť kupujúcemu vykonať penetračné testy vo svojom produkčnom prostredí.

I.2 Údaje o výrobe a prostredia

Dodávateľ nesmie používať produkčné údaje na testovacie činnosti.

Dodávateľ musí oddeliť vývojové, testovacie a produkčné prostredie (napr. siete, údaje, aplikácie a pod.)

I.3 Plán pre obnovenie činnosti po katastrofe.

Dodávateľ musí zriadiť a udržiavať plán obnovy po havárii a zabezpečiť jeho pravidelné testovanie.

Dodávateľ pri likvidácii zálohy bezpečne vymaže.

I.4 Údržba súvisiaca s bezpečnosťou

Pre akékoľvek bezpečnostné záplaty, ktoré dodávateľ zamýšľa nasadiť na službu XaaS/Cloud, dodávateľ použije a otestuje záplatu na testovacom prostredí. Až po úspešnom ukončení testovania na takom prostredí dodávateľ nasadí záplatu na produkčné prostredie.

I.5 Služby tretích strán

Dodávateľ musí informovať kupujúceho, ak sú do poskytovania služby zapojené alebo je v pláne zapojiť služby tretích strán (napr. služby dátových centier).

J PRÍSTUP A POUŽÍVANIE SYSTÉMOV A ZDROJOV KUPUJÚCEHO

Táto časť sa bude aplikovať iba v prípade, že kupujúci udelí dodávateľovi prístup a možnosť používať systémy kupujúceho na plnenie tejto zmluvy.

J.1 Fyzický

Ak kupujúci poskytuje prístup a/alebo prepojovacie zariadenie nainštalované v priestoroch dodávateľa, dodávateľ musí zabezpečiť, aby:

- sa kontrola fyzického prístupu používala v technickej oblasti, kde sa nachádza toto zariadenie; a
- fyzický prístup k týmto zariadeniam bol obmedzený na tých, ktorí potrebujú prístup k zariadeniu na plnenie zmluvy a sú autorizovaný dodávateľom.

J.2 Systémy kupujúceho

Dodávateľ :

- bude vstupovať do systémov kupujúceho a používať ich iba na poskytovanie predmetu dodávky;
- zabezpečí, aby prístup a prenos dát neboli zneužité na vykonanie útoku (napr. pri prenose dát, kontrola malvéru);
- bude dodržiavať spôsoby prístupu a pravidlá stanovené kupujúcim a poskytnuté dodávateľovi vopred (napr. rešpektovanie sieťových adries, ktoré pridelil kupujúci, dodržiavanie časov odozvy pre zdroje riadenia kupujúceho, ...);
- zabezpečí, aby každý, kto koná v mene dodávateľa a potrebuje používať systémy kupujúceho, bol riadne oprávnený dodávateľom a kupujúcemu boli poskytnuté identifikačné informácie; a
- zabezpečí, aby so systémami kupujúceho boli spojené iba riadne autorizované zdroje dodávateľa.

J.3 Zdroje dodávateľa

Ak sa na prístup a/alebo prepojenie so systémami kupujúceho používajú zdroje dodávateľa, dodávateľ musí:

- dodržiavať osvedčené bezpečnostné postupy na riadenie týchto zdrojov (napr. musí mať tieto zdroje aktualizované najnovšími bezpečnostnými záplatami, ako je antimalvérový softvér a záplaty operačných systémov a inštalovaný softvér, konfigurovať obmedzené práva pre užívateľov, konfigurovať obmedzené vykonávacie práva na odnímateľných médiách, zaviesť mechanizmy pre zamykanie relácie – session-locking na týchto zdrojoch po krátkej dobe nečinnosti, ...);
- zabezpečiť, aby zdroje (vrátane autentifikačných tokenov, mobilných zariadení a súvisiacich telefónnych čísel) boli vyhradené pre dodávateľa a používané len jeho zamestnancami a tretími stranami určenými na zabezpečovanie predmetu dodávky);
- zaviesť riadenie prístupu k sieti na zdrojoch dodávateľa používaných na výkon služby;
- zaviesť silný overovací systém (napr. dvojfaktorovú autentifikáciu) pre prístup k týmto zdrojom; a zabezpečiť sledovateľnosť využívania týchto zdrojov všetkými používateľmi;
- uchováva protokoly po dobu dohodnutú v NPA a/alebo objednávke vrátane súvisiacich dokumentov (napr. zmluva o zachovaní mlčanlivosti alebo zmluva o spracovaní údajov) alebo štandardne 6 mesiacov; a
- poskytnúť kupujúcemu na požiadanie výpisy z uchovaných protokolov.

V prípade, že kupujúci poskytuje dodávateľovi účty, je dodávateľ povinný:

- zabezpečiť sledovateľnosť priradenia a použitia účtu;
- uchovávať stopy po dobu dohodnutú v NPA a/alebo objednávke vrátane súvisiacich dokumentov (napr. zmluva o zachovaní mlčanlivosti alebo zmluva o spracovaní údajov) alebo štandardne 6 mesiacov; a
- poskytnúť kupujúcemu na požiadanie výpisy z uchovaných protokolov sledovania.

J.4 Systémy a aplikácie kupujúceho

V prípade, že kupujúci poskytuje dodávateľovi účty, je dodávateľ povinný:

- bezodkladne informovať kupujúceho, ak už účet nie je potrebný; a
- zabezpečiť, aby sa účty poskytované pre serverovú komunikáciu používali len na tento účel.

J.5 Správa zdrojov kupujúceho

V prípade, že kupujúci poskytuje dodávateľovi fyzické zdroje (softvér, hardvér, počítače, USB kľúče, odznak, tablet, smartfón, prístupové alebo prepojovacie zariadenie...) je dodávateľ povinný sledovať tieto zdroje. Po ukončení zmluvy je dodávateľ povinný vrátiť kupujúcemu zdroje, ktoré ešte má.

K ODBORNOSŤ A BEZPEČNOSŤ

K.1 Školenie na zvýšenie povedomia a vzdelávanie:

Dodávateľ je povinný zabezpečiť, aby jeho zamestnanci a všetky tretie strany určené na poskytovanie predmetu dodávky:

- mali príslušné bezpečnostné zručnosti (napr. na riadenie bezpečnostných incidentov); a
- boli oboznámení s obsahom a realizáciou platných bezpečnostných pravidiel.

K.2 Špecifické bezpečnostné pravidlá kupujúceho

Ak kupujúci poskytne pre vykonávanie odborných služieb špecifické bezpečnostné pravidlá, dodávateľ zabezpečí, aby boli jeho zamestnanci a určené tretie strany informované o takýchto pravidlách pred začatím akejkoľvek úlohy.

K.3 Subdodávatelia

Ak dodávateľ pri plnení zmluvy s kupujúcim používa subdodávateľov, dodávateľ ich konkrétne identifikuje ako subdodávateľov a zabezpečí, aby bola vždy uplatňovaná rovnaká náležitá starostlivosť.

K.4 Zaobchádzanie s citlivými časťami predmetu dodávky

Na požiadanie kupujúceho sa dodávateľ zaviaže, že bude používať iba pracovníkov preverených z hľadiska bezpečnosti, t.j. preverených štátnymi orgánmi, na spracovanie citlivých častí predmetu dodávky pred nasadením v sieti kupujúceho, ako aj na udržiavanie citlivých častí predmetu dodávky počas celej prevádzkovej fázy.

DEFINÍCIE A SKRATKY

Zmluva	znamená zmluvu, ktorú podpísal kupujúci s dodávateľom a obsahuje odkaz na túto ISA alebo Všeobecné podmienky nákupu spoločnosti Orange, v prípade ak nedochádza k uzatvoreniu písomnej zmluvy.
Aktíva	zahŕňajú primárne a podporné aktíva, ako sú definované v ISO/IEC 27005.
„Zadné vrátka“ (Back Doors).	znamená funkciu alebo poruchu predmetu dodávky, ktorá umožňuje podvodný neoprávnený prístup k údajom.
CVE	znamená bežné zraniteľnosti a odhalené miesta, ako sú definované v: http://CVE.Mitre.org/index.html .
CVSS	znamená systém posudzovania miery zraniteľnosti, ako je definovaný v http://www.first.org/cvss/ .
Chyba	znamená akúkoľvek odchýlku skutočnej kvality predmetu dodávky od kvality zamýšľanej zmluvou, napr. nedostatok, nesúlad predmetu dodávky s príslušnou špecifikáciou alebo neplnenie v súlade s príslušnou dokumentáciou.
Predmet dodávky	znamená akékoľvek zariadenie, HW, SW, produkt alebo službu objednanú v hlavnej zmluve, vrátane všetkých hlavných a vedľajších povinností.
Informačná bezpečnosť	znamená – v súlade s ISO/IEC 27001 a ISO/IEC 27005 - bezpečnosť v rozsahu spracovania informácií a činností (primárne aktíva), opierajúc sa o technické (vrátane, ale nielen, IT, priestory, vybavenie, siete) a netechnické zdroje (vrátane, ale nielen, podporné aktíva, ako sú zamestnanci, partneri, organizácie, postupy a podmienky).
internet vecí	znamená akékoľvek pripojené zariadenia alebo zariadenia pre internet vecí
Oficiálna oprava	znamená, že je k dispozícii kompletné riešenie dodávateľa na opravu zraniteľnosti, buď prostredníctvom oficiálnej záplaty alebo upgradu.
Objednávka	znamená objednávku, ktorú vystavil kupujúci.

Kupujúci	znamená Orange Slovensko, a. s.
Sieť kupujúceho	znamená sieť spravovanú kupujúcim a všetky súvisiace prístupové infraštruktúry siete kupujúceho potrebné na zabezpečenie komunikácie medzi zdrojmi každej strany.
Zdroje kupujúceho	znamená hardvér, softvér, služby, ktoré patria kupujúcemu a používajú sa na účely poskytovania predmetu dodávky.
Softvérový výsledok	označuje akýkoľvek softvér, ktorý je: (i) primárne založený na a/alebo zameraný na požiadavky a/alebo špecifikácie kupujúceho, poskytovaný kupujúcim alebo výlučne pre kupujúceho; a/alebo (ii) vyvinutý alebo implementovaný dodávateľom podľa tejto zmluvy (alebo akýchkoľvek následných dodatkov) a/alebo akékoľvek TSA a/alebo NPA a/alebo akákoľvek dodávka, a ktorý nie je podkladom; ktorý môže alebo nemusí byť chránený podľa práva duševného vlastníctva, ako aj akýkoľvek produkt alebo proces z neho vyplývajúci.
Vyhlásenie o zhode	znamená prílohu zmluvy s podrobnými technickými bezpečnostnými požiadavkami pre predmet dodávky.
Výkaz prác (SoW)	znamená dokument definujúci činnosti špecifické pre projekt, predmet dodávky a časový plán pre dodávateľa poskytujúceho predmet dodávky a/alebo služby kupujúcemu.
Zdroje dodávateľa	znamená hardvér, softvér, ktoré patria kupujúcemu alebo je za ne zodpovedný, a používajú sa na účely poskytovania predmetu dodávky.
Dočasná oprava	znamená, že je k dispozícii oficiálne, ale dočasné riešenie na opravu zraniteľnosti, vrátane – ale nie výlučne – dočasných rýchlych opráv, nástrojov alebo postupov.
Zraniteľnosť	znamená slabosť, ktorá znižuje dostupnosť, integritu alebo dôvernosť.
XaaS	znamená čokoľvek dodané používateľom ako služba vrátane SaaS (softvér ako služba), PaaS (platforma ako služba), IaaS (infraštruktúra ako služba) alebo podobnej.
Zero-Day	znamená neodhalená zraniteľnosť, ktorú hackeri môžu využiť na nepriaznivé ovplyvnenie predmetu dodávky. Je známy ako „zero-day“ (alebo „zero-hour“ alebo „0-day“ alebo „day zero“), pretože nie je verejne nahlásený alebo oznámený predtým, než sa stáva aktívny, takže dodávateľovi zostáva nula dní, počas ktorých má vytvoriť záplaty alebo odporučiť postupy na zmiernenie dôsledkov.

-koniec dokumentu-