# Príloha o informačnej bezpečnosti

- ďalej len „ISA“ -

## VŠEOBECNÉ ZÁSADY

Táto Príloha o informačnej bezpečnosti (ISA) ustanovuje opatrenia týkajúce sa informačnej bezpečnosti. Ak je to relevantné pre predmet dodávky uvedený v Zmluve, Dodávateľ musí považovať tieto opatrenia za minimálny bezpečnostný štandard a tieto opatrenia musia platiť počas trvania Zmluvy, bez ohľadu na to, či je predmet dodávky obstarávaný na základe Zmluvy alebo prostredníctvom jeho subdodávateľov.

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

## VŠEOBECNÉ UPLATNENIE ISA

Dodávateľ je povinný dodržiavať požiadavky ISA pre všetky zložky predmetu dodávky tak, ako sú definované v nasledujúcich bodoch:

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

## VŠEOBECNÉ UPLATNENIE ŠPECIFICKÝCH ČASTÍ TÝKAJÚCICH SA PREDMETU DODÁVKY

Nasledujúce časti platia pre akýkoľvek druh 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 podľa tabuľky A:

- **Časť D:** „Kryptografia a overovanie“
- **Časť E:** „Bezpečnosť už v štádiu návrhu (Security by design)“
- **Časť F:** „Oprava zraniteľností softvéru“
- **Časť G:** „Údaje kupujúceho v službách XaaS/cloudových službách“
- **Časť H:** „Kontrola prístupu v službách XaaS/cloudových službách“
- **Časť I:** „Operácie v službách XaaS/cloudových službách“
- **Časť J:** „Prístup k systémom a zdrojom kupujúceho a ich používanie“
- **Časť K:** „Profesionalita a bezpečnosť“

| Časť predmetu dodávky | Uplatňované časti |
|---|---|
| Softvér | A, B, C, D, E, F |
| Hardvér | A, B, C, D, E, F |
| Služby XaaS/cloudové služby | 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 poskytne dodávateľ kupujúcemu do 10 pracovných dní všetky informácie potrebné na posúdenie bezpečnosti predmetu dodávky ako napríklad bezpečnostný test/správy z auditu, skeny zraniteľnosti a analýzy robustnosti kódov.

## A.2 Politiky bezpečnosti

Dodávateľ je povinný uplatňovať podnikové politiky bezpečnosti informácií podľa normy ISO/IEC 27001 alebo obdobného postupu uznávaného v odvetví.

Ak je dodávateľ certifikovaný, je povinný poskytnúť 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 je povinný udržiavať takúto certifikáciu počas celého trvania jeho zmluvných povinností.

## A.3 Audit

Kupujúci má právo vykonávať audity s cieľom skontrolovať, či dodávateľ dodržiava bezpečnostné požiadavky kupujúceho definované v Zmluve.

## A.4 Tretie strany

Pokiaľ dodávateľ na poskytovanie predmetu dodávky kupujúcemu využíva tretie strany, dodávateľ je povinný zabezpečiť, aby takéto tretie strany spĺňali bezpečnostné opatrenia dohodnuté v Zmluve.

## A.5 Súlad s NESAS

POZNÁMKA: Tento odsek A.5 sa vzťahuje iba na zariadenia mobilnej siete (čo predstavuje zariadenia základnej mobilnej siete, RAN a mobilného prístupu).

Dodávatelia, ktorí ponúkajú zariadenia mobilnej siete, musia podstúpiť mechanizmus hodnotenia dodávateľa a procesov životného cyklu (Network Equipment Security Assurance Scheme, NESAS) podľa príslušných špecifikácií NESAS vydaných Asociáciou GSM (GSMA PRD FS.13/15/16) v aktuálnej verzii.

Dodávateľ zároveň musí spoločnosti Orange/DT poskytnúť správu z auditu a správu z hodnotenia, ktoré boli vyhotovené ako výstup z hodnotenia uskutočneného uznaným audítorom. Toto hodnotenie sa musí dokončiť pred ponúkaním akýchkoľvek zariadení mobilnej siete. V prípade opätovného posúdenia dodávateľa alebo predmetu dodávky dodávateľa sa poskytnú všetky aktualizované správy.

### A.6 Nedodržiavanie ISA

Pokiaľ sa dodávateľ dozvie o nedodržaní bezpečnostných opatrení v predmete dodávky, bezodkladne poskytne kupujúcemu analýzu situácie a plán nápravy. Ak kupujúci schváli plán nápravy, dodávateľ ho zrealizuje bez toho, aby kupujúcemu vznikli akékoľvek náklady, a dodávateľ poskytne dôkaz o účinnosti plánu nápravy.

Ak nedodržiavanie pretrváva, alebo plán nápravy nie je schválený alebo zlyhá, automaticky sa to bude považovať za závažné porušenie Zmluvy.

## B ORGANIZÁCIA BEZPEČNOSTI

### B.1 Štruktúra

Na požiadanie kupujúceho poskytne dodávateľ informácie o svojej organizácii bezpečnosti.

### B.2 Kontaktný bod

Dodávateľ vymenuje kontaktnú osobu pre záležitosti týkajúce sa bezpečnosti, ako aj kontaktnú osobu z vyššieho manažmentu alebo pracovníka pre starostlivosť o kľúčových zákazníkov na riešenie eskalačných záležitostí. Kontakty sa poskytnú pri každej objednávke a ich zmeny sa musia bezodkladne oznámiť.

### B.3 Bezpečnostné kontroly

Raz ročne, na žiadosť jednej alebo oboch zmluvných strán, dodávateľ a kupujúci zorganizujú stretnutie s cieľom skontrolovať bezpečnostné aspekty (napr. vývoj a naplánované operácie, ktoré môžu mať vplyv na bezpečnosť).

Každá zmluvná strana môže požiadať o mimoriadne bezpečnostné stretnutie, ktoré musí druhá zmluvná strana prijať, ak si situácia vyžaduje spoločnú analýzu alebo okamžité rozhodnutie (napríklad vážny incident alebo závažný vývoj hrozieb).

### B.4 Bezpečnostné opatrenia pre údaje kupujúceho

Údaje kupujúceho predstavujú akékoľvek aktíva kupujúceho ako obchodné informácie (napr. zmluvy alebo obchodné plány) alebo technické informácie (napr. schémy siete).

Dodávateľ je povinný zaviesť nasledujúce opatrenia pre zdieľané údaje kupujúceho, ktoré kupujúci klasifikoval ako dôverné, t. j. údaje, ktoré kupujúci zašifroval alebo označil ako dôverné:

- takéto údaje budú pri ukladaní a prenose zašifrované, a
- bude zavedený silný systém overovania (napr. systém dvojúrovňového overovania).

V prípade potreby výmeny šifrovaných informácií sa zmluvné strany vopred dohodnú na spôsobe výmeny.

## C RIADENIE INCIDENTOV

### C.1 Odhaľovanie (detection)

Dodávateľ musí mať zavedené opatrenia na odhaľovanie bezpečnostných incidentov, ktoré ovplyvňujú kupujúceho a ktoré sa vyskytujú v prostredí dodávateľa. Bezpečnostné incidenty zahŕňajú okrem iného stratu, zmenu, zverejnenie alebo neoprávnený prístup k údajom alebo informáciám kupujúceho alebo neoprávnené zverejnenie chráneného zdrojového kódu alebo iných práv duševného vlastníctva.

### C.2 Oznamovanie

Dodávateľ je povinný akýkoľvek takýto bezpečnostný incident okamžite oznámiť kupujúcemu.

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

Takéto oznámenie o bezpečnostnom incidente sa musí odoslať buď na adresu cert@orange.com alebo cert@telekom.de, a zároveň kontaktu dodávateľa na kupujúceho.

Podrobnosti o bezpečnostných incidentoch si dodávateľ uchová minimálne do ďalšej bezpečnostnej kontroly medzi zmluvnými stranami.

### C.3 Vyriešenie

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

### C.4 Pozastavenie prístupu dodávateľa k systémom kupujúceho

POZNÁMKA: Tento odsek C.4 sa nevzťahuje na softvérové časti predmetu dodávky, hardvérové časti predmetu dodávky, časti predmetu dodávky týkajúce sa zariadení zákazníka a služby XaaS/cloudové služby.

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

### C.5 Pozastavenie prístupu kupujúceho k službám XaaS/cloudovým službám

POZNÁMKA: Tento odsek C.5 sa nevzťahuje na softvérové časti predmetu dodávky, hardvérové časti predmetu dodávky, časti predmetu dodávky týkajúce sa zariadení zákazníka a odborné služby.

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

Pokiaľ kupujúci nie je schopný pozastaviť prístup, kupujúci výslovne požiada dodávateľa, aby pozastavil všetky prístupy kupujúceho až do vyriešenia incidentu. Dodávateľ musí takejto žiadosti okamžite vyhovieť.

### C.6 Správa o bezpečnosti služieb XaaS/cloudových služieb a odborných služieb

POZNÁMKA: Tento odsek C.6 sa nevzťahuje na softvérové časti predmetu dodávky, hardvérové časti predmetu dodávky a časti predmetu dodávky týkajúce sa zariadení zákazníka.

Kupujúci si môže od dodávateľa vyžiadať správu o bezpečnosti týkajúcu sa služieb XaaS/cloudových služieb a/alebo odborných služieb najviac dvakrát ročne. Táto správa o bezpečnosti musí okrem iného zahŕňať nasledujúce informácie:

- počet bezpečnostných incidentov zistených za posledných 12 mesiacov, jednotlivo pre interné a externé príčiny, ak je to relevantné; a
- podrobnosti o bezpečnostných incidentoch počas toho obdobia (čas odhalenia, povaha a dopad, vyriešenie, čas obnovy služby, čas uzavretia, čas nutný na vyriešenie).

## 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 a častiach predmetu dodávky týkajúcich sa zariadení zákazníka bude kupujúci môcť meniť a chrániť v súlade s najnovšími poznatkami. Pokiaľ ide o overovacie údaje a kryptografické kľúče, ktoré kupujúci nemôže meniť, dodávateľ poskytne kupujúcemu zoznam takýchto údajov a ich účel. Pri službách XaaS/cloudových službách sa táto požiadavka vzťahuje iba na overovacie údaje, ktoré kupujúci používa na ochranu svojich údajov, vrátane administrátorských účtov.

### D.2 Sila kryptografických algoritmov a kľúčov

Dodávateľ zavedie len štandardizované kryptografické algoritmy a dĺžky kľúčov odporúčané vládnymi inštitúciami (napríklad BSI, ANSSI a NIST) v čase uzavretia alebo obnovenia Zmluvy a takéto štandardizované kryptografické algoritmy a dĺžky kľúčov bude pravidelne primerane aktualizovať pri nových častiach predmetu dodávky.

# E BEZPEČNOSŤ UŽ V ŠTÁDIU NÁVRHU (SECURITY BY DESIGN)

## E.1 Posilnenie zabezpečenia

Dodávateľ využije osvedčené postupy na posilnenie zabezpečenia systému. To okrem iného 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), ktorý bude štandardne bezpečne nakonfigurovaný podľa postupov konfigurácie v súlade s najnovšími poznatkami (napríklad https://www.cisecurity.org). Okrem toho dodávateľ zabezpečí, aby predmet dodávky neobsahoval žiadne „zadné dvierka“ (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 voči neočakávaným vstupom, ako napríklad SQL Injection, predvídateľné správanie v situáciách preťaženia, atď.).

## E.3 Transparentnosť dokumentácie

Dodávateľ poskytne kupujúcemu:

- potrebnú dokumentáciu na bezpečnú konfiguráciu predmetu dodávky, pričom túto dokumentáciu bude priebežne aktualizovať;
- softvérový kusovník v strojovo čitateľnom formáte (vrátane názvu predajcu podľa potreby, názvu a verzie softvéru a/alebo open source softvéru), pričom bude tento zoznam priebežne aktualizovať.

## E.4 Doplňujúce opatrenia

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

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

# F OPRAVA ZRANITEĽNOSTÍ SOFTVÉRU

## F.1 Odhaľovanie (detection)

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

## F.2 Norma CVE

Podľa potreby bude mať každá zistená zraniteľnosť jedinečný identifikátor CVE spojený so skóre podľa CVSS (v3 alebo vyšší), ktorý pozostáva zo základu CVSS, časového skóre a identifikačné číslo vektora.

## F.3 Oznámenia

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

Dodávateľ je povinný oznamovať bezpečnostné upozornenia v akomkoľvek spracovateľnom formáte (napríklad CVRF, CSAF, XML, JSON) e-mailom:

| | |
|---|---|
| Všetky časti predmetu dodávky | cert@orange.com<br>cert@telekom.de |
| Časti predmetu dodávky týkajúce sa zariadení zákazníka | Tie isté adresy ako vyššie a:<br>devices.security@orange.com<br>equipmentsecurity@telekom.de |

### F.4 Dohoda o úrovni poskytovaných služieb na opravu 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 v3** | **Maximálny čas na poskytnutie dočasnej opravy** | **Maximálny čas na poskytnutie oficiálnej opravy** |
|---|---|---|
| Od vysokého po kritické **7,0 – 10,0** | 5 (päť) kalendárnych dní | 30 (tridsať) kalendárnych dní |
| Od nízkeho po stredné **0 – 6,9** | nevzťahuje sa | 6 (šesť) mesiacov |

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

### F.5 Udržiavanie bezpečnosti komponentov tretej strany

Dodávateľ zaistí, aby počas životného cyklu predmetu dodávky bola udržiavaná 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, môže kupujúci otvoriť údržbovú požiadavku na jej opravu. Okrem časti F.4 je dodávateľ povinný dodržiavať aj podmienky údržby na opravu chyby súvisiacej so zraniteľnosťou.

### F.7 Výnimky

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

- v prípadoch vyžadujúcich rýchlejšiu odozvu ako vo vyššie uvedenej tabuľke (napr. zverejnenie zraniteľnosti v určitej časti predmetu dodávky, ktorú používa kupujúci); a
- v technickom prostredí potrebnom na prevádzku predmetu dodávky (napr. operačný systém pre softvérovú časť predmetu dodávky).

### F.8 Náhrada škody/sankcie za opravy zraniteľnosti

Okrem opravných prostriedkov v dôsledku závažného porušenia, ako je uvedené v časti A.6 „ V prípade opätovného posúdenia dodávateľa alebo predmetu dodávky dodávateľa sa poskytnú všetky aktualizované správy.

Nedodržiavanie ISA“, si kupujúci môže voči dodávateľovi uplatniť náhradu škody alebo sankcie podľa častí Zmluvy „Náhrada škody“ alebo „Sankcie“.

V prípade zraniteľností sa uplatní nasledujúca schéma náhrady škody:

> Ak dodávateľ neposkytne bezpečnostnú oficiálnu opravu zraniteľností so skóre CVSS vyšším alebo rovnajúcim sa 7 podľa tabuľky uvedenej v časti F.4 „Dohoda o úrovni poskytovaných služieb na opravu zraniteľností“, náhrada škody sa vypočíta takto:
>
> **A = V x N / 300**
>
> **A**: suma náhrady škody.
>
> **V**: hodnota predmetu dodávky.
>
> **N**: počet kalendárnych dní nad rámec termínu dodania oficiálnej opravy.

### F.9 Údržba súvisiaca s bezpečnosťou

Pre každú časť predmetu dodávky dodávateľ určí minimálnu dobu podpory, ktorá nemôže byť kratšia ako záručná doba.

Počas životného cyklu predmetu dodávky dodávateľ poskytne kupujúcemu:

- aktuálne vydanie predmetu dodávky a jeho budúce vydania so všetkými bezpečnostnými opravami;
- bezpečnostné opravy po ich vydaní, pričom dodrží časy opráv zraniteľností definované v časti F.4;
- informácie (napr. CVE, skóre CVSS) o opravených zraniteľnostiach.

## G ÚDAJE KUPUJÚCEHO V SLUŽBÁCH XAAS/CLOUDOVÝCH SLUŽBÁCH

### G.1 Obmedzenie používania údajov kupujúceho

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

### G.2 Oddelenie údajov kupujúceho

Dodávateľ je povinný zabezpečiť oddelenie údajov kupujúceho od údajov ostatných zákazníkov dodávateľa.

### G.3 Dôverné údaje kupujúceho

Dodávateľ pri prenose a uložení zašifruje všetky údaje, ktoré kupujúci označí ako dôverné a ktoré sú uložené v službe XaaS/cloudovej službe dodávateľa.

### G.4 Šifrovacie mechanizmy dodávateľa

Ak kupujúci využíva na ochranu údajov kupujúceho mechanizmus šifrovania poskytnutý dodávateľom, dodávateľ zabezpečí, aby:

- takéto údaje boli pri ukladaní a prenose po celý čas zašifrované; a
- sa pre prístup k takýmto údajom používalo silné overovanie (napr. dvojúrovňové overovanie).

### G.5 Zaznamenávanie prístupov k údajom kupujúceho a ich používania

Dodávateľ je povinný:

- zaznamenávať prístup k údajom kupujúceho a ich používanie v službe XaaS/cloudovej službe, vrátane prístupu k týmto údajom a ich používania jeho zamestnancami a akýmikoľvek určenými tretími stranami; a
- uchovávať takéto záznamy po dobu dohodnutú v NPA a/alebo objednávke vrátane súvisiacich dokumentov (napr. zmluva o mlčanlivosti alebo zmluva o spracovaní údajov) alebo štandardne po dobu 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/cloudovej službe vo formáte a na obdobie vzájomne vopred dohodnuté s kupujúcim.

Podľa častí D.2 a G.4 sa na vrátenie údajov pre kupujúceho použijú iba šifrované pripojenia, pokiaľ kupujúci písomne nesúhlasil s výnimkou.

Na konci obdobia vrátenia údajov dodávateľ zničí všetky prostredia kupujúceho a údaje kupujúceho v službe XaaS/cloudovej službe takým spôsobom, ktorý znemožní prístup k takýmto údajom alebo ich čítanie.

Dodávateľ poskytne kupujúcemu potvrdenie o zničení.

## H KONTROLA PRÍSTUPU V SLUŽBÁCH XAAS/CLOUDOVÝCH SLUŽBÁCH

### H.1 Fyzická bezpečnosť

Dodávateľ poskytne fyzicky zabezpečené zariadenia tak pre produkčnú cloudovú infraštruktúru, ako aj pre umiestnenia na vzdialené operácie.

Je potrebné zaviesť minimálne tieto kontrolné mechanizmy:

- fyzický prístup vyžaduje oprávnenie a je sledovaný;
- každá osoba musí na pracovisku viditeľne nosiť oficiálnu identifikáciu;
- návštevníci musia podpísať záznam v evidencii návštev a musia byť v priestoroch pracoviska sprevádzaní a/alebo sledovaní; a
- držba kľúčov/prístupových kariet a možnosť prístupu na miesta sa monitoruje. Pracovníci, ktorí ukončujú pracovný pomer u dodávateľa, musia vrátiť kľúče/karty.

### H.2 Kontrola prístupu k systému a správa hesiel

Dodávateľ musí kontrolovať systémy služby tak, že obmedzí prístup iba na oprávnených pracovníkov.

Na komponentoch infraštruktúry a systémoch správy cloudu, ktoré sa používajú na prevádzku prostredia služieb dodávateľa, je dodávateľ povinný vynucovať politiku hesiel. Dodávateľ je povinný chrániť heslá pomocou bezpečných mechanizmov, ako napríklad digitálny trezor.

Dodávateľ zavedie kontrolu prístupu k systému a sledovanie účtov s cieľom zabezpečiť, aby k systémom mali prístup len schválení zamestnanci pre jednotlivé operácie a podporu. Kontrola prístupu k systému musí zahŕňať overovanie systému, oprávnenie, schválenie prístupu, poskytovanie a zrušenie pre zamestnancov a iných „používateľov“ definovaných dodávateľom.

### H.3 Prehodnotenie prístupových práv

Účty zamestnancov dodávateľa v sieti a operačnom systéme sa budú pravidelne prehodnocovať, aby sa zabezpečili vhodné úrovne prístupu pre zamestnancov.

Ak zamestnanec dodávateľa odíde zo zmluvného projektu, dodávateľ je povinný prijať okamžité opatrenia na zrušenie prístupu takýchto bývalých zamestnancov do siete, ako aj telefonického a fyzického prístupu.

### H.4 Bezpečnostná brána

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

Dodávateľ rozmiestni bezpečnostné brány, ktoré bude spravovať, na vykonávanie kontroly paketov s bezpečnostnými politikami konfigurovanými na filtrovanie paketov na základe protokolu, portu, zdroja a cieľovej adresy IP podľa potreby, s cieľom identifikovať overené zdroje, destinácie a typy prevádzky.

### H.5 Kontrola malvéru

Dodávateľ je povinný používať antimalvérový softvér na skenovanie nahrávaných súborov. Definície malvéru sa musia aktualizovať minimálne raz denne.

### H.6 Šifrovanie a vzdialené pripojenia k službám XaaS/cloudovým službám

Na prístup kupujúceho k službe XaaS/cloudovej službe a jej používanie musia byť použité iba šifrované pripojenia, pokiaľ kupujúci písomne neschváli výnimku.

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

V každom prípade musia byť podporované najnovšie dostupné prehliadače pre pripojenie k službám Xaas/cloudovým službám.

## I OPERÁCIE V SLUŽBÁCH XAAS/CLOUDOVÝCH SLUŽBÁCH

### I.1 Penetračné testy

Dodávateľ vyhodnotí bezpečnosť služby XaaS/cloudovej služby prostredníctvom penetračných testov aspoň raz ročne. Správu a plán zmiernenia z týchto testov musí poskytnúť kupujúcemu.

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

### I.2 Produkčné údaje a prostredia

Dodávateľ nesmie používať produkčné údaje na testovacie činnosti.

Dodávateľ je povinný oddeliť vývojové, testovacie a produkčné prostredia (napr. siete, údaje, aplikácie a pod.).

### I.3 Plán obnovy po havárii

Dodávateľ zriadi a bude udržiavať plán obnovy po havárii a zabezpečí jeho pravidelné testovanie.

Správu obsahujúcu výsledky z týchto testov musí na požiadanie poskytnúť kupujúcemu.

Pri likvidácii dodávateľ bezpečne vymaže zálohy.

### I.4 Údržba súvisiaca s bezpečnosťou

V prípade akýchkoľvek bezpečnostných opráv, ktoré dodávateľ zamýšľa nasadiť na službu XaaS/cloudovú službu, dodávateľ použije a otestuje opravu na testovacom prostredí. Dodávateľ nasadí opravu na produkčné prostredie až po úspešnom ukončení testovania na testovacom prostredí.

### I.5 Služby tretích strán

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

### I.6 Premiestňovanie údajov

Dodávateľ je povinný informovať kupujúceho, ak sa údaje kupujúceho (vrátane záloh) premiestnia do iného dátového centra, než bolo pôvodne schválené v Zmluve.

## J PRÍSTUP K SYSTÉMOM A ZDROJOM KUPUJÚCEHO A ICH POUŽÍVANIE

Táto časť sa uplatní iba ak kupujúci udelí dodávateľovi prístup do systémov kupujúceho a možnosť ich používania na účely plnenia Zmluvy.

### J.1 Fyzický prístup

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

- sa kontrola fyzického prístupu vykonávala v technickej oblasti, kde sa nachádzajú takéto zariadenia; a
- bol fyzický prístup k týmto zariadeniam obmedzený na tie osoby, ktoré potrebujú k zariadeniam prístup na účely plnenia Zmluvy a ktoré majú riadne oprávnenie od dodávateľa.

### J.2 Systémy kupujúceho

Dodávateľ je povinný:

- pristupovať k systémom kupujúceho a používať ich iba na poskytovanie predmetu dodávky;
- zabezpečiť, aby prístup a prenos údajov neboli zneužité na vykonanie útoku (napr. vykoná kontrolu malvéru pri prenose údajov);
- 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 atď.);
- zabezpečiť, aby každá osoba, ktorá koná v mene dodávateľa a potrebuje používať systémy kupujúceho, bola riadne oprávnená dodávateľom a kupujúcemu boli poskytnuté identifikačné informácie; a
- zabezpečiť, aby so systémami kupujúceho boli spojené iba riadne autorizované zdroje dodávateľa.

### J.3 Zdroje dodávateľa

Ak sa na prístup k systémom kupujúceho a/alebo prepojenie so systémami kupujúceho používajú zdroje dodávateľa, dodávateľ je povinný:

- dodržiavať osvedčené bezpečnostné postupy na riadenie týchto zdrojov (napr. musí mať tieto zdroje aktualizované najnovšími bezpečnostnými opravami, ako sú antimalvérový softvér a opravy operačných systémov a inštalovaný softvér, konfigurovať obmedzené práva pre užívateľov, konfigurovať obmedzené vykonávacie práva na vymeniteľných médiách, zaviesť mechanizmy pre zamykanie relácie (session-locking) na týchto zdrojoch po krátkej dobe nečinnosti atď.);
- 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 kontrolu prístupu k sieti na zdrojoch dodávateľa používaných na vykonávanie služieb;

- zaviesť silný overovací systém (napr. dvojúrovňové overovanie) na prístup k týmto zdrojom; a zabezpečiť sledovateľnosť využívania týchto zdrojov všetkými používateľmi;
- uchovávať protokoly po dobu dohodnutú v NPA a/alebo objednávke vrátane súvisiacich dokumentov (napr. zmluva o mlčanlivosti alebo zmluva o spracúvaní údajov) alebo štandardne 6 mesiacov; a
- na požiadanie poskytnúť kupujúcemu výpisy z uchovávaných protokolov.

Ak kupujúci poskytuje dodávateľovi účty, je dodávateľ povinný:

- zabezpečiť sledovateľnosť priradenia a používania účtu;
- uchovávať záznamy zo sledovania po dobu dohodnutú v NPA a/alebo objednávke vrátane súvisiacich dokumentov (napr. zmluva o mlčanlivosti alebo zmluva o spracúvaní údajov) alebo štandardne 6 mesiacov; a
- poskytnúť kupujúcemu na požiadanie výpisy z uchovaných záznamov sledovania.

### J.4 Systémy a aplikácie kupujúceho

Ak kupujúci poskytuje dodávateľovi účty, je dodávateľ povinný:

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

### J.5 Správa zdrojov kupujúceho

Ak kupujúci poskytuje dodávateľovi fyzické zdroje (softvér, hardvér, počítače, USB kľúč, prístupovú kartu, tablet, smartfón, prístupové alebo prepojovacie zariadenie atď.), je dodávateľ povinný na tieto zdroje dohliadať. Po ukončení Zmluvy je dodávateľ povinný vrátiť zdroje kupujúceho, ktoré má ešte v držbe.

## K PROFESIONALITA 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 vhodné 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 pred začatím akejkoľvek úlohy boli jeho zamestnanci a všetky určené tretie strany informované o takýchto pravidlách.

### K.3 Subdodávatelia

Ak dodávateľ na plnenie Zmluvy s kupujúcim využíva subdodávateľov, dodávateľ ich musí konkrétne identifikovať ako subdodávateľov a zabezpečí, aby sa vždy uplatňovala rovnaká náležitá starostlivosť.

### K.4 Zaobchádzanie s citlivými časťami predmetu dodávky

Na požiadanie kupujúceho a na základe dohody v NPA sa dodávateľ zaviaže, že bude využívať iba pracovníkov preverených z hľadiska bezpečnosti, t. j. preverených štátnymi orgánmi, na nakladanie s citlivými časťami predmetu dodávky pred nasadením v sieti kupujúceho, ako aj na údržbu citlivých častí predmetu dodávky počas celej prevádzkovej fázy.

## L DODÁVANIE AKTUALIZÁCIÍ SOFTVÉRU

POZNÁMKA: táto časť sa uplatňuje iba na časti predmetu dodávky týkajúce sa zariadení zákazníka.

Dostupnosť aktualizácie softvéru zo strany dodávateľa počas obdobia podpory príslušnej časti predmetu dodávky (pozri časť F.9) musí byť bez dodatočných poplatkov tak pre kupujúceho, ako aj pre koncového používateľa.

Dodávateľ je povinný bezodkladne poskytnúť aktualizáciu softvéru (napríklad ako image súbor celého firmvéru, aktualizácia v rámci jednej aplikácie a pod.) prostredníctvom akéhokoľvek mechanizmu podľa Zmluvy hneď ako sa identifikuje v softvéri predmetu dodávky zraniteľnosť a v súlade s časťou F.4.

Pred dodaním akejkoľvek aktualizácie softvéru je dodávateľ povinný dodržať postup dohodnutý s kupujúcim.

Dodanie bezpečnostnej opravy musí využívať technický prístup v súlade s najnovšími poznatkami (inovácia firmvéru zariadenia, aktualizácie aplikácií prostredníctvom obchodov s aplikáciami a pod.) s cieľom opraviť zraniteľnosť na všetkých zraniteľných zariadeniach.

V súvislosti s časťou F.4 je pre časti predmetu dodávky, ktoré používajú operačný systém Android, dodávateľ povinný poskytovať pravidelné aktualizácie pri zachovaní úrovne bezpečnostných opráv (Security Patch Level, SPL) príslušnej časti predmetu dodávky v rámci obdobia 90 (deväťdesiat) dní (alebo akéhokoľvek kratšieho obdobia, ktoré sa vyžaduje na certifikáciu takýchto častí predmetu dodávky) počas celého životného cyklu produktu.

### DEFINÍCIE A SKRATKY

| | |
|---|---|
| **Zmluva** | znamená akúkoľvek zmluvu, ktorú podpísal kupujúci s dodávateľom a obsahuje odkaz na túto ISA. |
| **Aktíva** | zahŕňajú primárne a podporné aktíva, ako sú definované v norme ISO/IEC 27005. |
| **Správa z auditu** | znamená dokument, v ktorom sú uvedené výsledky auditu týkajúceho sa predmetu dodávky vedeného tímom audítorov, podľa definície GSMA *"FS.13 - Network Equipment Security Assurance Scheme – Overview"*. |
| **Zadné dvierka (Back Door)** | znamenajú funkciu alebo poruchu predmetu dodávky, ktorá umožňuje podvodný neoprávnený prístup k údajom. |
| **CVE** | znamená bežné zraniteľnosti a odhalené miesta (Common Vulnerabilities and Exposures) podľa tejto definície: http://cve.mitre.org/index.html. |
| **CVSS** | znamená systém posudzovania miery zraniteľnosti (Common Vulnerability Scoring System) podľa tejto definície: http://www.first.org/cvss/. |
| **Chyba** | znamená akúkoľvek odchýlku skutočnej kvality predmetu dodávky od kvality stanovenej v zmluve, napr. nedostatok, nesúlad predmetu dodávky s príslušnou špecifikáciou alebo neplnenie v súlade s príslušnou dokumentáciou. |
| **Predmet dodávky** | znamená akékoľvek zariadenie, produkt a/alebo službu objednanú na základe hlavnej Zmluvy, vrátane všetkých hlavných a vedľajších povinností. |
| **Správa z hodnotenia** | znamená zdokumentované hodnotenie vytvorené bezpečnostným testovacím laboratóriom NESAS<br>úrovne súladu príslušnej časti predmetu dodávky s príslušnou<br>špecifikáciou záruky bezpečnosti definovanou organizáciou pre normalizáciu 3GPP, podľa definície GSMA *"FS.13 - Network Equipment Security Assurance Scheme – Overview"*. |
| **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 (okrem iného najmä IT, priestory, vybavenie, siete) a netechnické zdroje (okrem iného najmä podporné aktíva ako zamestnanci, partneri, organizácie, postupy a podmienky). |
| **Internet vecí (Internet of Things)** | znamená akékoľvek pripojené zariadenia alebo vybavenie pre internet vecí. |
| **Životný cyklus** | znamená obdobie vrátane záručnej lehoty, obdobia podpory a akéhokoľvek predĺženého obdobia podpory produktu. |
| **NPA** | znamená zmluvu uzatvorenú pridruženou spoločnosťou spoločnosti Orange podľa Rámcovej zmluvy spoločnosti BuyIn alebo spoločnosti Orange, prípadne uzatvorenú spoločnosťou |

| | |
|---|---|
| | BuyIn. Termín NPA sa zhoduje s termínmi „Realizačná zmluva“, „Zmluva špecifická pre projekt“ a „Projektová zmluva“; akékoľvek ustanovenie, v ktorom sa používa termín „NPA“, sa vzťahuje aj na tieto druhy zmlúv. |
| **Oficiálna oprava** | znamená, že je k dispozícii kompletné riešenie dodávateľa na opravu zraniteľnosti, a to buď prostredníctvom oficiálnej opravy alebo inovácie. |
| **Objednávka** | znamená nákupnú objednávku vystavenú kupujúcim. Termín „objednávka“ zodpovedá termínu „nákupná objednávka“ použitému v Zmluvách uzatvorených spoločnosťou Orange a jej pridruženými spoločnosťami. Akékoľvek ustanovenie, v ktorom sa používa termín „objednávka“, sa bude rovnakým spôsobom vzťahovať na termín „nákupná objednávka“. |
| **Kupujúci** | znamená Orange Slovensko, a.s. Akékoľvek ustanovenie stanovené pre kupujúceho sa bude rovnakým spôsobom vzťahovať na termín „objednávajúca zmluvná strana“. |
| **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 a služby, ktoré patria kupujúcemu a používajú sa na účely poskytovania predmetu dodávky. |
| **Softvérový kusovník (Software Bill of Materials, SBoM)** | znamená podľa definície normy ISO/IEC 27036 zoznam softvérových komponentov, subkomponentov a väzieb so súvisiacimi informáciami. |
| **Softvérový výsledok** | znamená akýkoľvek softvér, ktorý je:<br>(i) primárne založený na a/alebo zameraný na požiadavky a/alebo špecifikácie kupujúceho, poskytovaný kupujúcim alebo výlučne pre kupujúceho; a/alebo<br>(ii) vyvinutý alebo implementovaný dodávateľom podľa tejto Zmluvy (alebo akýchkoľvek následných dodatkov k nej) a/alebo akejkoľvek TSA a/alebo NPA a/alebo akejkoľvek dodávky, a ktorý nie je podkladom;<br>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 na predmet dodávky. |
| **Výkaz prác** | 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 dodávateľovi alebo za ne dodávateľ zodpovedá, a ktoré sa používajú na účely poskytovania predmetu dodávky. |
| **Obdobie podpory** | znamená obdobie, počas ktorého sa dodávateľ zaväzuje poskytovať podporu pre predmet dodávky vrátane bezpečnostných opráv. Toto obdobie podpory nesmie byť kratšie ako obdobie ustanovené v príslušných právnych predpisoch alebo obdobie dohodnuté v Zmluve, podľa toho, ktoré z nich je dlhšie. |
| **Dočasná oprava** | znamená, že je k dispozícii oficiálne, ale dočasné riešenie na opravu zraniteľnosti, okrem iného vrátane dočasných rýchlych opráv, nástrojov alebo postupov. |
| **Zraniteľnosť** | znamená nedostatok, ktorý znižuje dostupnosť, integritu alebo dôvernosť. |
| **XaaS** | znamená čokoľvek, čo sa dodáva používateľom ako služba, vrátane SaaS (softvér ako služba), PaaS (platforma ako služba), IaaS (infraštruktúra ako služba) alebo podobné riešenie. |
| **Zero-Day** | znamená nezverejnenú zraniteľnosť, ktorú môžu hekeri využiť na nepriaznivé ovplyvnenie predmetu dodávky. Nazýva sa „zero-day“ (alebo „zero-hour“ alebo „0-day“ alebo „day zero“), pretože nie je verejne nahlásená alebo oznámená predtým, než sa stáva aktívnou. Dodávateľovi teda zostáva nula dní, počas ktorých má vytvoriť opravy alebo odporučiť postupy na zmiernenie jej dôsledkov. |

**- koniec dokumentu -**