# Aneks Informacijske Sigurnosti (Information Security Annex)

- u daljnjem tekstu: „ISA” -

## OSNOVNA NAČELA

Ovaj aneks Informacijske Sigurnosti (u daljnjem tekstu: ISA) uspostavlja mjere informacijske sigurnosti HT grupe. Ako je primjenjivo na Isporuke navedene u Ugovoru, Dobavljač mora uzeti u obzir ove mjere kao minimalni sigurnosni standard i mora ih prihvatiti za vrijeme trajanja Ugovora, neovisno o tome jesu li Isporuke nabavljene prema Ugovoru ili putem treće strane.

Ove mjere pokrivaju različite aspekte informacijske sigurnosti, a primjenjuju se ovisno o prirodi Isporuka na koje se odnosi Ugovor.

Osim toga, ove mjere mogu se pojačati dodatnim sigurnosnim mjerama koje će odrediti Naručitelj i koje su dogovorene između stranaka u dokumentima priloženim Sporazumu, PA i / ili Narudžbi.

## PRIORITET DOKUMENATA

Ovaj ISA je standardni dokument koji se odnosi na sve Sporazume sklopljene s Dobavljačem koji upućuju na ovaj ISA.

Primjenjuje se sljedeće:

1. Ugovor će prevladati nad ISA-om, osim ako nije drugačiji redoslijed prednosti naveden u Ugovoru; i
2. Bez obzira na gore navedeno, svi pojmovi napisani velikim slovima tumače se prema definicijama na kraju ovog ISA i prema zadanim postavkama definiranim u Ugovoru koji sadrži referencu na ovu ISA-u.

Stranke su suglasne da će ovaj ISA prevladavati nad dokumentima dobavljača koji definiraju sigurnosne mjere priložene ili navedene u Ugovoru, PA i / ili Narudžbi.

## OPĆA PRIMJENJIVOST ISAA

Dobavljač mora udovoljavati zahtjevima ISAa za sve isporuke kako je definirano u sljedećem:

- **Softver** se odnosi na softverske proizvode dobavljača i / ili prilagođeni softver koji proizlazi iz Sporazuma koje su ugovorne strane dogovorile (npr. softverske isporuke);
- **Hardver** uključujući bilo koji ugrađeni softver / firmware (npr. IT oprema, mrežna oprema i dr.);
- **Korisnička oprema** uključujući bilo koji ugrađeni softver/firmware (npr. oprema za krajnje korisnike, mobilni telefoni, mobilni širokopojasni uređaji, tableti, uređaji povezani s krajnjim korisnikom, mobilni CPE, mobilni uređaji za Internet stvari, povezani satovi, pametni TV, pristupnici, set- gornje kutije, repetitori itd.);
- **XaaS / Cloud** usluge (npr. Softver kao usluga); i
- **Profesionalne usluge** za obavljanje instalacije, obuke i edukacije, integracije, održavanja i / ili savjetovanje.

## PRIMJENJIVOST POSEBNIH ODJELJAKA U ODNOSU NA ISPORUKE

Sljedeći odjeljci primjenjuju se na bilo koju vrstu Isporuka:

**- Odjeljak A**: "Poštivanje ugovora i standarda"

**- Odjeljak B**: "Organizacija sigurnosti"

**- Odjeljak C**: "Upravljanje incidentima"

Slijedeći odjeljci primjenjuju se prema prirodi isporuka kako je definirano u tablici A:

- **Odjeljak D**: "Kriptografija i autentifikacija"

- **Odjeljak E**: "Sigurnost u dizajnu"

- **odjeljak F**: "Rješavanje softverskih ranjivosti"

- **odjeljak G**: "Podaci Naručitelja u XaaS / Cloud usluzi "

- **Odjeljak H**: "Kontrola pristupa XaaS / Cloud usluga "

- **Odjeljak I**: "Upravljanje XaaS / Cloud uslugama"

- **Odjeljak J**: "Pristup i korištenje sustava i resursa Naručitelja"

- **Odjeljak K**: "Profesionalci i sigurnost"

-**Odjeljak L:** „Distribucija ažuriranja software-a“

| Isporuka | Primjenjivi odjeljci |
|---|---|
| **Softver** | **A, B, C, D, E, F** |
| **Hardver** | **A,B, C, D, E, F** |
| **XaaS/Cloud usluge** | **A, B,C, D, E, F, G, H, I** |
| **Korisnička oprema** | **A, B, C, D, E, F, L** |
| **Profesionalne usluge** | **A, B, C, J, K** |

**Tabica A: Primjenjivost odjeljaka ISAa**

# A POŠTIVANJE UGOVORA I STANDARDA

## A.1 Procjena sigurnosti isporučenih proizvoda

Dobavljač će na zahtjev naručitelja dostaviti Naručitelju u roku od 10 radnih dana sve potrebne informacije za procjenu sigurnosti isporučenih proizvoda, kao što su sigurnosni testovi / revizijska izvješća, skeniranja ranjivosti i analiza robusnosti koda.

## A.2 Sigurnosne politike

Dobavljač će primijeniti politiku sigurnosti kompanije u skladu s normom ISO / IEC 27001 ili sličnom praksom priznatom u industriji.

Ako je Dobavljač certificiran, dostaviti će sigurnosne certifikate Naručitelju te ga obaviještavati o obnovi ili oduzimanju svojih certifikata.

Ako je Naručitelj odabrao Dobavljača na temelju certifikata (npr. ISO / IEC 27001), Dobavljač je obvezan zadržati taj certifikat tijekom cijelog trajanja ugovora.

### A.3 Revizija

Naručitelj i/ili HT Grupa ima pravo obavljati reviziju Dobavljača uz prethodnu najavu kako bi provjerili usklađenost Dobavljača s uvjetima sigurnosti Naručitelja a kako je definirano u Ugovoru.

### A.4. Treće strane

U slučaju da Dobavljač koristi treće strane za Isporuke Naručitelju, Dobavljač će osigurati da takve treće strane ispune sigurnosne mjere dogovorene u Sporazumu.

### A.5 NESAS usklađenost

Napomena: Ovaj A.5 odlomak primjenjiv je isključivo za opremu za mobilne mreže (znači opremu za mobilnu jezgrenu mrežu, radio pristupnu mrežu i opremu za mobilni pristup).

Dobavljači koji nude opremu za mobilne mreže moraju proći kroz NESAS (Network Equipment Security Assurance Scheme) procjenu razvoja i životnog ciklusa dobavljača, a kako je definirano u odgovarajućim NESAS specifikacijama, a koje je objavila GSM Association (GSMA PRD FS.13/15/16), u njihovoj aktualnoj verziji.

Dodatno, dobavljač mora Naručitelju dostaviti revizorsko izvješće kao i sažetak izvješća procjene, koja su kreirana kao rezultat procjene, provedene od strane priznatog revizora. Procjena mora biti dovršena prije nego što se ponudi bilo kakva oprema za mobilnu mrežu. Ako se Dobavljač ili Isporučivi proizvodi Dobavljača ponovno procijene, Dobavljač će dostaviti sva ažurirana izvješća.

### A.6 Nepoštivanje ovog ISA

U slučaju da dobavljač postane svjestan nesukladnosti sa sigurnosnim mjerama u njegovim Isporukama, Dobavljač će odmah dostaviti Naručitelju analizu situacije i plan rješavanja uočenih nesukladnosti. Ako Naručitelj prihvati plan rješavanja, Dobavljač će ga implementirati bez ikakvih troškova prma Naručitelju te Dobavljač mora dokazati učinkovitost plana rješavanja.

Ako se neusklađenost nastavi ili plan rješavanja nesukladnosti nije prihvaćen ili ne uspije, to će se automatski smatrati materijalnim kršenjem Ugovora.

## B ORGANIZACIJA SIGURNOSTI

### B.1 Struktura

Dobavljač će na zahtjev naručitelja dostaviti podatke o svojoj organizaciji sigurnosti.

### B.2 Točka kontakta

Dobavljač će imenovati kontakt osobu za pitanja vezana uz sigurnost kao i kontakt iz višeg menadžmenta ili voditelja ključnog računa za rješavanje pitanja eskalacije. Za svaku Narudžbu treba osigurati kontakte, a promjene će se odmah komunicirati.

### B.3 Sigurnosni pregledi

Jednom godišnje, na zahtjev jedne ili obiju stranaka, Dobavljač i Naručitelj će organizirati sastanak kako bi provjerili sigurnosne aspekte (npr. promjene i planirane aktivnosti koje mogu utjecati na sigurnost).

Svaka stranka može zatražiti izvanredni sigurnosni sastanak koji će druga stranka prihvatiti ako situacija nameće zajedničku analizu ili neposrednu odluku (primjerice, veliki incident ili značajna evolucija sigurnosnih prijetnji).

### B.4 Sigurnosne mjere za podatke Naručitelja

Podaci Naručitelja su bilo koja imovina Naručitelja, poput poslovnih informacija (npr. ugovori ili poslovni planovi) ili tehničkih informacija (npr. mrežni dijagrami).

Dobavljač će implementirati sljedeće mjere za podatke koje Naručitelj klasificira povjerljivima, npr. podaci koji su kriptirani od strane Naručitelja i/ili označeni kao povjerljivi:

- takvi podaci moraju biti kriptirani pri pohranjivanju i prenošenju; i
- jaki sustav autentikacije (npr. 2 faktorska autentikacija) mora biti implementiran.

Stranke će unaprijed dogovoriti o načinu razmjene u slučaju potrebe za razmjenom kriptiranih informacija.

## C UPRAVLJANJE INCIDENTIMA

### C.1 Otkrivanje

Dobavljač mora imati uspostavljene mjere za otkrivanje sigurnosnih incidenata koji utječu na Naručitelja, a koji se javljaju u okruženju Dobavljača. Sigurnosni incidenti uključuju, ali nisu ograničeni na gubitak, izmjenu, otkrivanje ili neovlašten pristup podacima ili informacijama Naručitelja i neovlašteno otkrivanje vlasničkog izvornog koda ili drugih prava intelektualnog vlasništva.

### C.2 Obaviještavanje

Dobavljač će odmah obavijestiti Naručitelja u slučaju bilo kojeg takvog sigurnosnog incidenta.

Ako se utvrdi kršenje i / ili zloupotreba podataka ili informacija Naručitelja, Dobavljač će obavijestiti Naručitelja prema važećim propisima, ali najkasnije u roku od 24 sata.

Takva obavijest o sigurnosnom incidentu bit će poslana na cert@t.ht.hr i kontakt osobu Naručitelja koja je navedena u Ugovoru s Dobavljačem.

Dobavljač će sačuvati podatke o sigurnosnim incidentima najmanje do sljedećeg sigurnosnog pregleda između stranaka.

### C.3 Rješavanje

Dobavljač mora uložiti najveći mogući napor da odmah riješi sigurnosne incidente te obavijestiti Naručitelja o rješavanju i završetku incidenta.

### C.4 Obustavljanje pristupa Dobavljača sustavima Naručitelja

NAPOMENA: Ovaj odjeljak C.4 ne odnosi se na Softver, Hardver, Korisničku opremu i XaaS / Cloud usluge.

U slučaju sigurnosnih incidenata u vezi s Profesionalnim uslugama, Naručitelj može obustaviti pristup Dobavljaču na sustave Naručitelja sve dok se incident ne riješi.

### C.5 Obustava pristupa Naručitelja Xaas / Cloud uslugama

NAPOMENA: Ovaj odjeljak C.5 ne odnosi se na Softver, Hardver, Korisničku opremu i Profesionalne usluge.

U slučaju sigurnosnog incidenta koji se odnosi na XaaS / Cloud usluge (npr. Upada u sustav, zlonamjerni softver), Naručitelj može obustaviti pristup navedenoj Usluzi sve dok se incident ne riješi.

U slučaju kada Naručitelj ne može obustaviti pristup, Naručitelj će Izričito zatražiti od Dobavljača da obustavi sve mogućnosti pristupa Naručitelja sve dok se incident ne riješi. Dobavljač mora odmah udovoljiti takvom zahtjevu.

### C.6 Sigurnosno izvješće za XaaS / Cloud usluge i profesionalne usluge

NAPOMENA: Ovaj odjeljak C.6 ne odnosi se na Softverske, Hardverske i isporuke Korisničke opreme.

Naručitelj može zatražiti od Dobavljača sigurnosno izvješće koje se odnosi na XaaS / Cloud usluge i / ili Profesionalne usluge najviše dvaput godišnje. Ovo sigurnosno izvješće uključuje, ali nije ograničeno na sljedeće podatke:

- broj sigurnosnih incidenata otkrivenih tijekom posljednjih 12 mjeseci, zasebno za unutarnje i vanjske uzroke ako je relevantno; i
- pojedinosti sigurnosnih incidenata tijekom razdoblja (vrijeme otkrivanja, priroda i utjecaj, rješavanje, vrijeme obnavljanja usluge, vrijeme zatvaranja, potrebno vrijeme rješavanje).

## D KRIPTOGRAFIJA I AUTENTIFIKACIJA

### D.1 Izmjena podataka autentifikacije i kriptografskih ključeva od strane Naručitelja

Svi podaci za provjeru autentičnosti i kriptografski ključevi (npr. Certifikati, parovi ključeva, simetrični ključevi, lozinke) u Softveru, Hardveru i isporučenoj Korisničkoj opremi moraju biti izmijenjivi od strane Naručitelja i zaštićeni u skladu s najboljim praksama. Za autentifikacijske podatke i kriptografske ključeve koje Naručitelj ne može mijenjati, Dobavljač će dostaviti popis takvih podataka i njihovu svrhu Naručitelju. Za usluge XaaS / Cloud, taj se uvjet primjenjuje samo na podatke za provjeru autentičnosti koje koristi Naručitelj radi zaštite svojih podataka uključujući i administratorske račune.

### D.2 Snaga kriptografskih algoritama i ključeva

Dobavljač će implementirati samo standardizirane kriptografske algoritme i duljine kriptografskih ključeva preporučene od strane vladinih institucija (kao što su npr. BSI, ANSSI i NIST) u trenutku sklapanja ili obnavljanja Ugovora te će redovito ažurirati takve standardizirane kriptografske algoritme i duljine ključeva u skladu s tim za nove Isporuke.

## E SIGURNOST U DIZAJNU

### E.1 Hardening

Dobavljač će primjeniti najbolje prakse hardeninga sustava. To uključuje, ali se ne ograničava na ograničavanje pristupa protokolima, uklanjanje ili onemogućavanje nepotrebnog softvera, mrežnih portova i usluga, uklanjanje nepotrebnih datoteka, korisničkih računa, ograničavanje dozvola za datoteke, upravljanje zakrpama i logiranje.

Dobavljač će osigurati Isporuke (uključujući i komponente i usluge treće strane) koji su zadano konfigurirani prema najsuvremenijim sigurnosnim konfiguracijskim praksama (kao što je npr. https://www.cisecurity.org/).

Osim toga, dobavljač će osigurati da Isporuke ne sadrže stražnje ulaze (Backdoors).

### E.2 Ispitivanje softverskih propusta

Dobavljač će testirati isporuke kako bi se osiguralo da one nemaju opasnih softverskih propusta navedenih u "CWE / SANS Top 25" (http://cwe.mitre.org) i / ili "OWASP TOP 10" (http://www.owasp.org) na datum isporuke (npr. robusnost prema neočekivanim ulazima kao što je SQL Injection, predvidljivo ponašanje u situacijama preopterećenja itd.).

### E.3 Transparentnost dokumentacije

Dobavljač će Naručitelju osigurati:

- potrebnu dokumentaciju za sigurnu konfiguraciju Isporuka i održavati tu dokumentaciju ažurnom;
- Troškovnik softvera u strojno čitljivom formatu (uključujući ime dobavljača ako je primjenjivo, naziv i verziju softvera i/ili otvorenog izvornog koda) i održavati takav inventar ažurnim.

### E.4 Dodatne mjere

Na zahtjev Naručitelja, ugovorne stranke mogu se međusobno dogovoriti o dodatnim sigurnosnim mjerama koje Isporuke moraju zadovoljiti.

Ove dodatne mjere mogu se prikupiti u dokumentu pod nazivom "Izjava o sigurnosnoj usklađenosti" (Security Statement of Compliance) i biti uključene u Sporazum i / ili u PA.

## F ISPRAVLJANJE SOFTVERSKIH RANJIVOSTI

### F.1 Otkrivanje

Dobavljač mora imati mjere za kontinuirano praćenje vanjskih sigurnosnih izvora (poput kooperativnih sigurnosnih testova, vanjskih istraživanja sigurnosti, otkrivanja open source ranjivosti ...) i praćenja ranjivosti koje bi mogle utjecati na Isporuke (uključujući i komponente trećih strana).

### F.2 Standard CVE

Gdje je prikladno, svaka ranjivost koju je otkrio Dobavljač mora imati jedinstveni CVE identifikator povezan s CVSS rezultatom (v3 ili više), a koja se sastoji od CVSS osnove, privremenog rezultata i vektora itd.

### F.3 Obavijesti

Dobavljač će odmah obavijestiti Naručitelja o svakoj ranjivosti (s CVSS rezultatom jednaki ili većim od 7,0), uključujući ranjivosti nultog dana (Zero-Day) koji utječu na Isporuke i njegove posljedice (npr. CVE ako postoji, rezultat CVSS-a, pogođene komponente ili usluge).

Dobavljač će komunicirati sigurnosne preporuke u formatu pogodnom za parsiranje (npr. CVRF, CSAF, XML, JSON), putem elektroničke pošte na adresu cert@t.ht.hr.

### F.4 Sporazum o razini usluge za rješavanje ranjivosti

Za svaku ranjivost koja utječe na Isporuke, Dobavljač će:

- poduzeti sve napore kako bi osigurao privremeni ispravak (Temporary fix) dostupan Naručitelju prema sljedećoj tablici; i
- poduzeti sve napore kako bi osigurao službeni ispravak (Official fix) dostupan Naručitelju prema sljedećoj tablici.

| CVSS base score v3 | Maksimalno vrijeme za osiguravanje privremenog ispravka | Maksimalno vrijeme za osiguravanje službenog ispravka |
|---|---|---|
| **7.0-10.0** | 5 (pet) kalendarskih dana | 30 (trideset) kalendarskih dana |
| **0-6.9** | Nije primjenjivo | 6 (mjeseci) mjeseci |

Vremenski brojač započinje kada se pronađe ranjivost, osim ranjivosti koja se nalazi na komponentama treće strane, gdje brojač vremena počinje kada je dostupan ispravak.

### F.5 Sigurnosno održavanje komponenti treće strane

Dobavljač mora osigurati da se komponente treće strane korištene u Isporukama sigurnosno održavaju tijekom životnog ciklusa Isporuka.

### F.6 Sigurnosni nedostaci

Dobavljač prihvaća da za svaku ranjivost koja utječe na Isporuke i otkrije ju Naručitelj tijekom ugovorenog razdoblja održavanja i / ili jamstvenog roka, Naručitelj može otvoriti nalog (ticket) za održavanje kako bi se ispravila. Dodatno uz odjeljak F.4, Dobavljač će poštivati uvjete održavanja kako bi se ispravio nedostatak koji je vezan za ranjivost.

### F.7 Izuzeci

Dobavljač će upotrijebiti ekonomski razumne napore kako bi podržao Naručitelja kod rješavanje Ranjivosti:

- u slučajevima koji zahtijevaju brži odgovor od gore navedene tablice (npr. javno objavljene ranjivosti u Isporukama koje koristi Naručitelj); i
- u tehničkom okruženju potrebno za upravljanje Isporukama (npr. operativni sustav za softverske Isporuke).

### F.8 Naknade štete / kazne za ispravke ranjivosti

Osim pravnih lijekova kao posljedica materijalne povrede navedene u odjeljku A.6 "Nepridržavanje sa ISA", Naručitelj može primijeniti naknadu štete ili kazne Dobavljaču prema odjeljcima "Naknada štete" ili "Kazne" Sporazuma.

U slučaju ranjivosti primjenjuje se sljedeća shema naknade štete:

Ako Dobavljač ne dostavi sigurnosni Službeni ispravak za ranjivosti s CVSS rezultatom većim od 7 prema tablici definiranoj u odjeljku F.4 " Sporazum o razini usluge za rješavanje ranjivosti ", naknada šteta izračunava se na sljedeći način:

**A = V x N / 300**

**A:** iznos naknade štete**.**

**V:** vrijednost Isporuke**.**

**N:** broj kalendarskih dana koji premašuju službeni rok za popravljanje**.**

### F.9 Sigurnosno održavanje

Dobavljač će za svaku Isporuku definirati minimalno razdoblje podrške koje ne može biti kraće od jamstvenog razdoblja.

Tijekom životnog ciklusa Isporuka, Dobavljač će Naručitelju osigurati:

- trenutno izdanje Isporuka i buduća izdanja sa svim sigurnosnim zakrpama
- sigurnosne zakrpe kada i kako se objavljuju, poštujući vremena rješavanja ranjivosti utvrđenih u odjeljku F.4.
- informacije (npr. CVE, CVSS rezultat) o ranjivostima koje su ispravljene dostavljenim zakrpama.

## G PODACI DOBAVLJAČA U XAAS/CLOUD USLUGAMA

### G.1 Ograničenje upotrebe podataka Naručitelja

Dobavljač će upotrebljavati podatke Naručitelja koji se prenose, obrađuju, generiraju i / ili pohranjuju u XaaS / Cloud usluzi samo za pružanje navedene usluge

### G.2 Razdvajanje podataka Naručitelja

Dobavljač mora provesti razdvajanje podataka Naručitelja od podataka drugih klijenata Dobavljača.

### G.3 Povjerljivi podaci Naručitelja

Dobavljač mora u prijenosu i kod pohrane kriptirati sve podatke koji je Naručitelj označio povjerljivima i koji su pohranjeni u Dobavljačevom XaaS/Cloud Service.

### G.4 Mehanizmi kriptiranja Dobavljača

U slučaju da Naručitelj koristi mehanizam kriptiranja koji osigurava Dobavljač radi zaštite podataka Naručitelja, Dobavljač će osigurati:

- da se ovi se podaci moraju kriptirati kod prijenosa i pohrane; i

- da se za pristup takvim podacima upotrebljava jaka autentikacija (npr. Autentikacija s dva faktora „two factor authentication“).

### G.5 Evidentiranje pristupa i korištenja podataka Naručitelja

Dobavljač će:

- bilježiti (logirati) pristup i korištenje podataka Naručitelja u XaaS / Cloud uslugama, uključujući njegove zaposlenike i bilo koje ovlaštene treće strane; i

- zadržati takve zapise za vremenski period dogovoren u PA i / ili Narudžbi, uključujući povezane dokumente (npr. Ugovor o neotkrivanju „Non-Disclosure Agreement“ ili Sporazum o obradi podataka „Dana Processing Agreement“) ili na rok od najmanje 6 mjesec ako drukčije nije definirano.

Izvadci zadržanih evidencija dostavljaju se Naručitelju na njegov zahtjev.

### G.6 Povrat podataka Naručitelja

Nakon raskida PA-a i / ili Narudžbe, Dobavljač će Naručitelju omogućiti povrat svih podataka Naručitelja u XaaS-u / Cloud servisu u formatu i za vremensko razdoblje koje je unaprijed dogovoreno s Naručiteljom.

Kao u odjeljcima D.2 i G4, samo će se kriptirane veze koristiti za povrat podataka od strane Naručitelja, osim ako se Naručitelj i Dobavljač pismenim putem ne dogovore drugačije.

Na kraju razdoblja povrata podataka, Dobavljač će uništiti sve Naručiteljeve okoline i podatke Naručitelja u XaaS / Cloud usluzi na način koji osigurava da im se ne više može pristupiti ili ih pročitati.

Dobavljač će naručitelju dostaviti potvrdu o uništenju podataka.

# H KONTROLA PRISTUPA XAAS/CLOUD USLUGAMA

## H.1 Fizička sigurnost

Dobavljač će osigurati fizički osigurane objekte za produkcijsku infrastrukturu usluga u oblaku kao i za lokacije za udaljene operacije.

Kontrole moraju obuhvatiti najmanje:

- fizički pristup koji zahtijeva autorizaciju i monitorira se;
- svatko mora jasno nositi službenu identifikaciju dok je na licu mjesta;
- posjetitelji moraju potpisati registar posjetitelja i biti praćeni i / ili promatrani u objektu; i
- prati se posjed ključeva / pristupnih kartica i mogućnost pristupa lokacijama. Zaposlenici koji prestaju raditi kod Dobavljača moraju vratiti ključeve / pristupne kartice.

## H.2 Kontrola pristupa sustavu i upravljanje lozinkama

Dobavljač će kontrolirati svoje usluge ograničavanjem pristupa samo ovlaštenim osobama.

Dobavljač će provoditi pravila o lozinkama na infrastrukturnim komponentama i sustavima za upravljanje oblakom koji se koriste za upravljanje uslugom Dobavljača. Dobavljač će štititi lozinke pomoću sigurnih mehanizama kao što je digitalni trezor.

Dobavljač će provoditi kontrolu pristupa sustavu, a odgovornost je osmišljena kako bi se osiguralo da samo odobreni operatori i zaposlenici za podršku imaju pristup sustavu. Kontrola pristupa sustavu uključuje provjeru autentičnosti, autorizaciju, odobrenje pristupa, pribavljanje i opoziv za zaposlenike i sve ostale "korisnike" definirane od strane Dobavljača.

## H.3 Pregled korisničkih prava pristupa

Računi (accounts) mrežnih i operativnih sustava zaposlenika Dobavljača redovito će se pregledavati kako bi se osigurala odgovarajuća razina pristupa zaposlenicima.

U slučaju da zaposlenik Dobavljača napusti ugovoreni projekt, Dobavljač mora poduzeti hitne korake kako bi ukinuo mrežni, telefonski i fizički pristup tim bivšim zaposlenicima.

## H.4 Sigurnosni pristupni uređaji

Dobavljač će koristiti sigurnosne pristupne uređaje (npr. vatrozidove, usmjerivače, reverzne proxy poslužitelje) za kontrolu pristupa između interneta i usluga Dobavljača dopuštajući samo autorizirani promet.

Implementirani sigurnosni pristupni uređaji moraju omogućavati inspekcije paketa prema sigurnosnim pravilima konfiguriranima za filtriranje paketa na temelju protokola, porta, izvorne i odredišne IP adrese prema potrebi, kako bi se identificirali ovlašteni izvori, odredišta i vrste prometa.

### H.5 Kontrole protiv zlonamjernog softvera

Dobavljač će koristiti softver za zaštitu od zlonamjernih programa za skeniranje prenesenih datoteka. Definicije zlonamjernog softvera ažuriraju se najmanje dnevno.

### H.6 Kriptiranje i udaljeno povezivanje s XaaS / Cloud uslugama

Za Naručiteljev pristup i korištenje XaaS / Cloud usluga moraju se koristiti kriptirane veze, osim ako Naručitelj ne dogovori iznimku u pisanom obliku.

Za treće strane koje djeluju u ime Dobavljača, Dobavljač će osigurati da se koriste samo autentificirane i kriptirane veze za udaljeni pristup podacima Naručitelja koji su obrađeni i / ili pohranjeni u XaaS / Cloud usluzi.

U svim slučajevima, najnoviji dostupni preglednici moraju biti podržani za povezivanje s Xaas / Cloud uslugama.

## I OPERATIONS OF XAAS/CLOUD SERVICES

### I.1 Penetracijska testiranja

Dobavljač će procijeniti sigurnost XaaS / Cloud usluge koristeći penetracijska testiranja najmanje jednom godišnje. Izvješće tih testova i plan rješavanja pronađenih nedostataka podijelit će s Naručiteljem.

Bez obzira na gore navedeno, Dobavljač će Naručitelju omogućiti XaaS/Cloud penetracijsko testiranje na njegovoj produkcijskoj okolini.

### I.2 Produkcijski podaci i okoline

Dobavljač ne smije koristiti produkcijske podatke za testne aktivnosti.

Dobavljač će odvojiti razvojne, ispitne i produkcijske okoline (npr. mreže, podatke, aplikacije itd.).

### I.3 Plan za oporavak od katastrofe

Dobavljač će uspostaviti i održavati plan oporavka od katastrofe i osigurati testiranje istog u redovitim intervalima.

Izvješće koje uključuje rezultate takvih testiranja Dobavljač će podijeliti s Naručiteljem na njegov zahtjev.

Dobavljač će na siguran način izbrisati sigurnosne kopije nakon prestanka potrebe za istima.

### I.4 Sigurnosno održavanje

Za svaku sigurnosnu zakrpu koju Dobavljač namjerava implementirati na Xaas / Cloud uslugu, Dobavljač će istu prethodno implementirati i testirati na testnom okruženju. Tek nakon uspješnog završetka testiranja na testnom okruženju, Dobavljač će implementirati zakrpu u produkcijskom okruženju.

### I.5 Usluge trećih strana

Dobavljač će obavijestiti Naručitelja ako su usluge trećih strana uključene ili će biti uključene u pružanje usluga Dobavljača (npr. usluge podatkovnih centara).

### I.6 Preseljenje/Prebacivanje podataka

Dobavljač će obavijestiti Naručitelja ako se Naručiteljevi podaci trebaju prebaciti u drugi data centar (uključujući i backup) od onoga koji je izvorno definiran u Ugovoru.

## J PRISTUP I KORIŠTENJE NARUČITELJEVIH SUSTAVA I RESURSA

Ovaj odjeljak primjenjivat će se samo ako Naručitelj odobri Dobavljaču pristup i korištenje sustava Naručitelja za izvršavanje Ugovora.

### J.1 Fizički pristup

Ako Naručitelj osigurava pristup i / ili opremu za interkonekciju instaliranu kod Dobavljača, Dobavljač mora osigurati:

- kontrolu fizičkog pristupa koja se primjenjuje na tehničko lokaciju gdje se takva oprema nalazi; i

- fizički pristup takvoj opremi ograničen je na one koji trebaju pristupiti opremi za provedbu Sporazuma i propisno su ovlašteni od strane Dobavljača.

### J.2 Sustavi Dobavljača

Dobavljač će:

- pristupati i upotrebljavati sustave Naručitelja samo za osiguravanje Isporuka;

- osigurati da se pristup i prijenos podataka ne koriste za izvršavanje napada (npr. za prijenos podataka, provjera zlonamjernog softvera);

- pridržavati se procedura za pristup i pravila koja je odredio Naručitelj, a koja su prethodno dostavljena Dobavljaču (npr. poštivanje mrežnih adrese koje je dodijelio Naručitelj, poštivanje vremena odziva Naručitelja, Naručiteljvo upravljanje resursima,...);

- osigurati da svatko tko djeluje u ime Dobavljača, a koji treba koristiti sustave Naručitelja, bude propisno ovlašten od strane Dobavljača, a identifikacijske informacije dostavljene Naručitelju; i

- osigurati da su samo propisno ovlašteni resursi Dobavljača povezani sa sustavima Naručitelja.

### J.3 Sustavi i aplikacije Naručitelja

Ako Naručitelj osigurava korisničke račune (accounts) Dobavljaču, Dobavljač će:

- odmah obavijestiti Naručitelja kada korisnički račun više nije potreban; i

- osigurati da se korisnički računi za poslužiteljske komunikacije koriste isključivo u tu svrhu.

### J.4 Upravljanje resursima Naručitelja

Ako Naručitelj osigurava fizičke resurse (softver, hardver, računala, USB stick, ID iskaznice/značke, tablet, pametni telefon, opremu za pristup ili međusobno povezivanje …) Dobavljaču, Dobavljač će voditi evidenciju o takvim resursima. Po prestanku Ugovora, Dobavljač će vratiti takve resurse Naručitelja koji su još uvijek u njegovom posjedu.

## K PROFESIONALCI I SIGURNOST

### K.1 Obuka i podizanje svijesti

Dobavljač će osigurati da njegovi zaposlenici i bilo koja treća strana ovlaštena za osiguravanje Isporuka:

- posjeduju odgovarajuće sigurnosne vještine (npr. za upravljanje sigurnosnim incidentima); i

- da su upoznati sa sadržajem i implementacijom primjenjivih sigurnosnih pravila.

### K.2 Specifična pravila sigurnosti Naručitelja

Ako Naručitelj ima specifična pravila sigurnosti za obavljanje profesionalnih usluga, Dobavljač će osigurati da njegovi zaposlenici i bilo koje ovlaštene treće strane budu obaviještene o takvim pravilima prije početka bilo kakvih poslova.

### K.3 Podugovaratelji

Ako Dobavljač koristi podugovaratelje za ispunjavanje Ugovora s Naručiteljem, Dobavljač će ih posebno identificirati kao podizvođače i osigurati da se i kod njih uvijek primjenjuje ista pažnja.

### K.4 Rukovanje osjetljivim Isporukama

Na zahtjev Naručitelja, Dobavljač se obvezuje da će koristiti samo osoblje koje je sigurnosno provjereno, tj. provjereno od strane odgovarajućih državnih institucija i agencija, za rukovanje osjetljivim Isporukama prije postavljanja u mrežu Naručitelja, kao i za održavanje osjetljivih Isporuka tijekom cijele operativne faze.

### K.5 Rukovanje podacima Naručitelja

Dobavljač će osigurati da njegovi zaposlenici i sve treće strane koje imaju pristup podacima Naručitelja prođu sigurnosnu provjeru prošlosti (npr. provjeru kaznene evidencije).

## L DISTRIBUCIJA AŽURIRANJA SOFTVERA

NAPOMENA: ovaj se odjeljak odnosi samo na Isporuke vezano uz Korisničku opremu.

Dostupnost ažuriranja softvera od strane Dobavljača unutar razdoblja podrške (vidi F.9) isporučenog proizvoda bit će besplatna za Naručitelja, kao i za krajnjeg korisnika.

Dobavljač će odmah isporučiti ažuriranje softvera (kao što je npr. cijeli firmware image file, ažuriranje jedne aplikacije, itd.) korištenjem bilo kojeg mehanizma koji je postavljen u Ugovoru čim se identificira sigurnosna ranjivost u softveru isporučenog proizvoda u skladu s odjeljkom F.4.

Dobavljač će poštovati proces dogovoren s Naručiteljem prije distribucije bilo kojeg novog ažuriranja softvera.

Distribucija sigurnosne zakrpe koristit će najsuvremeniji tehnički pristup (nadogradnje firmware-a uređaja, ažuriranja aplikacija putem trgovina aplikacijama(app stores), ….) kako bi se ranjivost popravila na svim ranjivim uređajima.

U vezi s odjeljkom F.4, za isporučene proizvode koje pokreće operativni sustav Android, Dobavljač mora osigurati redovita ažuriranja održavajući razinu sigurnosne zakrpa (SPL) isporučenih proizvoda u roku kraćem od 90 (devedeset) dana (ili bilo kojem kraćem razdoblju zatraženom za certifikaciju takvih isporučenih proizvoda) tijekom cijelog životnog ciklusa proizvoda.

## DEFINICIJE I SKRAĆENICE

| | |
|---|---|
| **Sporazum** | označava bilo koji ugovor Naručitelja s Dobavljačem s referencom na ovaj ISA. |
| **Imovina** | obuhvaća osnovnu i dodatnu imovinu definiranu u ISO / IEC 27005. |
| **Stražnji ulaz (BackDoor)** | znači značajku ili nedostatak isporučenih proizvoda koji omogućuje skriveni neovlašteni pristup podacima. |

| | |
|---|---|
| **CVE** | znači Common Vulnerabilities and Exposures kako je definirano u: http://cve.mitre.org/index.html |
| **CVSS** | znači Common Vulnerability Scoring System kao što je definirano u http://www.first.org/cvss/ |
| **Nedostatak** | označava svako odstupanje stvarne kvalitete Isporuke od ugovorene kvalitete, npr. nepoštivanje performansi isporučenih proizvoda u odnosu na njihovu odgovarajuću specifikaciju ili njihovu nemogućnost funkcioniranja na način specificiran u pripadajućoj dokumentaciji. |
| **Isporuke** | označava bilo koju opremu, proizvod i / ili uslugu naručenu preko glavnog ugovora, uključujući sve glavne i dodatne obveze. |
| **Informacijska sigurnost** | - u skladu s ISO / IEC 27001 i ISO / IEC 27005 - sigurnost u obradi informacija i djelatnosti (primarna imovina) oslanjajući se na tehničke (uključujući, ali ne ograničavajući se na IT, prostore, objekte, mreže) i netehničke resurse (uključujući, ali ne ograničavajući se na, ostala sredstva kao što su osoblje, partneri, organizacije, postupci, uvjeti i odredbe). |
| **Internet stvari** | znači sve povezane uređaje ili opremu za Internet stvari |
| **PA** | PA odgovara pojmovima "Sporazum o provedbi", "Sporazum o projektu" i "Ugovor o projektu", „Project Specific Agreement“ ili sl. : sve odredbe koje koriste izraz "PA" primjenjuju se i na te vrste ugovora ili dodataka ugovoru. |
| **Službeni ispravak** | znači da je dostupno kompletno rješenje Dobavljača za ispravak ranjivosti, bilo putem službene zakrpe ili nadogradnje. |
| **Narudžba** | označava narudžbenicu koju je izdao Naručitelj. "Narudžba" odgovara izrazu "Narudžbenica" u Ugovorima koji su sklopili HT i njegove Povezane tvrtke. Svaka odredba koja koristi izraz "Narudžba" primjenjuje se na "Narudžbenicu" na isti način. |
| **Naručitelj** | znači HT ili pridruženo društvo kao stranka PA ili Narudžbe. "Kupac" odgovara pojmu "Naručitelj" u Ugovorima koje je sklopila tvrtka HT i njegove povezane tvrtke. Svaka odredba koja je predviđena za Naručitelja u ovom Aneksu primjenjuje se na "Kupac" na isti način. |
| **Mreža Naručitelja** | znači mrežu kojom upravlja Naručitelj i svu povezanu infrastrukturu pristupa mreži Naručitelja potrebnu za osiguravanje komunikacija između resursa svake strane. |
| **Resursi Naručitelja** | znači hardver, softver, usluge koje pripadaju Naručitelju i koriste se u svrhu pružanja Isporuka. |
| **Software Result** | znači bilo koji softver koji je:<br>(i) prvenstveno na temelju Naručiteljevih zahtjeva i / ili specifikacije proizveden/osiguran isključivo za Naručitelja i / ili<br>(ii) razvijen ili implementiran od strane Dobavljača prema Ugovoru (i / ili bilo kojim naknadnim izmjenama i dopunama) i / ili PA i / ili bilo koje Narudžbe;<br>koji može ili ne mora biti zaštićen pravima intelektualnog vlasništva, kao i bilo koji proizvod ili postupak koji proizlazi iz njega. |
| **Izjava o primjenjivosti** | znači dodatak Sporazumu s detaljnim tehničkim sigurnosnim zahtjevima o Isporukama. |
| **Statement of Work (SoW)** | označava dokument koji određuje aktivnosti specifične za projekt, isporuke i rokove za koji Dobavljač pruža isporučene proizvode i / ili usluge Naručitelju. |
| **Resursi Dobavljača** | znači hardver, softver koji pripada i / ili je pod odgovornošću Dobavljača i koristi se u svrhu pružanja Isporuka. |

| | |
|---|---|
| **Privremeni ispravak** | znači da postoji službeni, ali privremeni ispravak koji je dostupan za popravak ranjivosti, uključujući - ali ne ograničavajući se na - privremene hitne ispravke, alate ili zaobilazna rješenja. |
| **Vulnerability** | znači ranjivost koja smanjuje dostupnost, integritet ili povjerljivost. |
| **XaaS** | znači bilo što isporučeno korisnicima kao uslugu, uključujući SaaS (Software as a Service), PaaS (platformu kao uslugu), IaaS (Infrastruktura kao servis) ili slično. |
| **Nulti dan (Zero-Day)** | znači neotkrivenu ranjivost koju hakeri mogu iskoristiti za nepovoljan utjecaj na isporuke. Poznat je kao "nulti dan" (ili "nula-satni" ili "0-dnevni" ili "dan O") jer nije javno prijavljen ili objavljen prije nego što postaje aktivan, ostavljajući dobavljaču nula dana za stvaranje zakrpe ili rješenja za ublažavanje posljedica te renjivosti. |

**- kraj dokumenta -**