Anex Informacijske Sigurnosti

- u daljnjem tekstu: „Anex” -

OSNOVNA NAČELA

Ovaj Anex Informacijske Sigurnosti (u daljnjem tekstu: Anex) 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, bez obzira na to jesu li Isporuke nabavljene Ugovorom 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 Kupac i koje su dogovorene između stranaka u dokumentima priloženim Sporazumu, PA i / ili Narudžbi.

PRIORITET DOKUMENATA

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

Primjenjuje se sljedeće:

1. Ugovor će prevladati nad Anexom, 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 Anexa i prema zadanim postavkama definiranim u Ugovoru koji sadrži referencu na ovu ISA.

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

OPĆA PRIMJENJIVOST ANEXA

Dobavljač mora udovoljavati zahtjevima Anexa 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. opremu krajnjih korisnika, uređaji za Internet stvari, informatička oprema itd.);
- **XaaS / Cloud** usluge (npr. Softver kao usluga); i
- **Profesionalne usluge** za obavljanje instalacije, obuke, integracije, održavanja i / ili savjetovanje.

PRIMJENJIVOST POSEBNIH ODJELJAKA U ODNOSU NA ISPORUKE

Sljedeći odjeljci primjenjuju se na bilo koju vrstu isporuke od strane dobavljača:

- 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 prema 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"

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**
Profesionalne usluge	**A, B, C, J, K**

Tabica A: Primjenjivost odjeljaka Anexa

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, on će dostaviti 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 ima pravo obavljati reviziju 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 Nepoštivanje ovog Anexa

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 Naručitelju te Dobavljač mora dokazati učinkovitost plana rješavanja.

Ako neusklađenost i dalje postoji postoji ili plan za rješavanje nije prihvaćen ili ne uspije, to će automatski postati materijalno kršenje 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 Pregled sigurnosti

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

Dobavljač će implementirati sljedeće mjere za podatke koje naručitelj klasificira povjerljivima:

- svi podaci moraju biti kriptirani pri pohranjivanju i prenošenju; i
- jaki sustav autentikacije (npr. 2 faktor autentikacija).

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

C UPRAVLJANJE INCIDENTIMA

C.1 Otkrivanje

Dobavljač mora imati uspostavljene mjere za otkrivanje sigurnosnih incidenata koji utječu na Naručitelja i 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.

C.2 Obaviještavanje

Dobavljač će odmah obavijestiti Naručitelja u slučaju 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.

Dobavljač će sačuvati podatke o sigurnosnim incidentima najmanje do sljedećeg pregleda sigurnosti 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, isporuke Hardvera 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, isporuke Hardvera 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 i hardverske isporuke.

Kupac 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 kupca

Svi podaci za provjeru autentičnosti i kriptografski ključevi (npr. Certifikati, parovi ključeva, simetrični ključevi, lozinke) u softveru i isporučivom softveru moraju biti izmijenjivi od strane Naručitelja i zaštićeni u skladu s najboljim praksama. Za autentifikacijske podatke i kriptografske ključeve koje kupac 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.

D.2 Snaga kriptografskih algoritama i ključeva

Dobavljač će implementirati samo standardizirane kriptografske algoritme preporučene od strane vladinih institucija (kao što su npr. BSI, ANSSI i NIST) u trenutku sklapanja ili obnavljanja Ugovora.

E SIGURNOST PREMA DIZAJNU

E.1 Hardening

Dobavljač će primjeniti standardizirane prakse hardeninga sustava. To uključuje ograničavanje pristupa protokolima, uklanjanje ili onemogućavanje nepotrebnog softvera, mrežnih portova i usluga, uklanjanje nepotrebnih datoteka, korisničkih računa, ograničavanje dozvola za datoteke, upravljanje zakrpama i zapisivanje.

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/).

Bez obzira na gore navedeno, Dobavljač će osigurati Naručitelju sve potrebne informacije kako bi sigurno konfigurirali i koristili Isporuke te osigurati da se takve informacije uvijek ažuriraju tijekom trajanja Ugovora.

Osim toga, dobavljač će osigurati da isporučivi proizvodi 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 Dodatne mjere

Na zahtjev Naručitelja, ugovorne stranke mogu se međusobno dogovoriti o dodatnim sigurnosnim mjerama koje Dobavljač mora 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 (v2 ili više). Svaka alternativa mora biti dogovorena u pisanom obliku s Naručiteljem.

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).

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 kupcu prema sljedećoj tablici; i

- poduzeti sve napore kako bi osigurao službeni ispravak (Official fix) dostupan Kupcu prema sljedećoj tablici.

CVSS base score v2	Maksimalno vrijeme za osiguravanje privremenog ispravka	Maksimalno vrijeme za osiguravanje službenog ispravka
7.0-10.0	7 (sedam) 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 su komponente treće strane korištene u Isporukama sigurnosno održavane tijekom razdoblja održavanja ili usluge koje je Naručitelj ugovorio.

F.6 Sigurnosni nedostaci

Dobavljač prihvaća da za svaku ranjivost koja utječe na Isporuke i otkrije ju kupac tijekom ugovorenog razdoblja održavanja i / ili jamstvenog roka, da kupac 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 isporuci koju koristi kupac); 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.5 "Nepridržavanje ove 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: V je vrijednost Isporuke**.**

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

F.9 Sigurnosno održavanje

Tijekom ugovorenog razdoblja održavanja i / ili jamstvenog roka, Dobavljač će osigurati da softverske i hardverske isporuke i sljedeća izdanja budu isporučena sa svim sigurnosnim zakrpama. Sigurnosne zakrpe se mogu isporučiti ili primijeniti kao zaseban paket.

Tijekom životnog ciklusa Isporuke, Dobavljač će osigurati sigurnosne zakrpe Naručitelju kada i kako se objavljuju, poštujući vremena rješavanja ranjivosti utvrđenih u odjeljku F.4.

Dobavljač će pružiti informacije (npr. CVE, CVSS rezultat) Naručitelju o ranjivostima koje su ispravljene dostavljenim zakrpama.

G PODACI DOBAVLJAČA U XAAS/CLOUD USLUGAMA

G.1 Ograničenje upotrebe podataka o kupcima

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

G.2 Razdvajanje podataka o kupcima

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

G.3 povjerljivi podaci kupca

Dobavljač mora u prijenosu i kod pohrane kriptirati sve podatke koji je naručitelj označio povjerljivima.

G.4 Mehanizmi kriptiranja Dobavljača

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

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

- da se za pristup takvim podacima upotrebljava se jaka autentifikacija (npr. Autentikacija s dva faktora).

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 vrijeme dogovoreno u PA i / ili Narudžbi, uključujući povezane dokumente (npr. Ugovor o otkrivanju ili Sporazum o obradi podataka) ili najmanje 6 mjeseci kao zadana postavka.

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 dogovorene s Naručiteljom.

Kao u odjeljku G4, samo će se šifrirane 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 sadržavati 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 pristupnih prava

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 Kupca 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 penetracijsko testiranje na 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 da se testira u redovitim intervalima.

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

I.4 Sigurnosno održavanje

Za svaku sigurnosnu zakrpu koju je Dobavljač namjerava implementirati na Xaas / Cloud uslugu, Dobavljač će primijeniti i testirati sigurnosnu zakrpu na testnom okruženju. Tek nakon uspješnog završetka ispitivanja na takvom okruženju, Dobavljač će implementirati zakrpu u produkcijskom okruženju.

I.5 Usluge trećih strana

Dobavljač će obavijestiti Naručitelja ako su usluge trećih strana uključene ili planirane da budu uključene u davanje usluga Dobavljača (npr. usluge podatkovnih centara).

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 međusobno povezivanje opremi instaliranoj kod Dobavljača, Dobavljač mora osigurati:

- kontrolu fizičkog pristupakoja se primjenjuje na tehničko područje 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, provjeru zlonamjernog softvera);

- pridržavati se sredstava za pristup i pravila koja je odredio Naručitelj i prethodno su dostavljeni Dobavljaču (npr. poštujte mrežne adrese koje je dodijelio Naručitelj, poštuju vrijeme kupca za resurse za upravljanje kupcima ...);

- osigurati da svatko tko djeluje u ime Dobavljača koji treba koristiti sustave Kupca 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 račun više nije potreban; i

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

J.4 Upravljanje resursima kupca

Ako Naručitelj osigurava fizičke resurse (softver, hardver, računala, USB stick, značku, tablet, pametni telefon, opremu za pristup ili međusobno povezivanje …), 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 će se i kod njih uvijek primjenjivati 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 nacionalne vlasti, za rukovanje osjetljivim Isporukama prije postavljanja u mrežu Naručitelja, kao i za održavanje osjetljivih Isporuka tijekom cijele operativne faze.

DEFINICIJE I SKRAĆENICE

Sporazum	označava bilo koji ugovor Naručitelja s Dobavljačem s referencom na ovaj Anex.
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: (i) prvenstveno na temelju Naručiteljevih zahtjeva i / ili specifikacije proizveden/osiguran isključivo za kupca i / ili (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; 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 kupcu.
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 -