European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

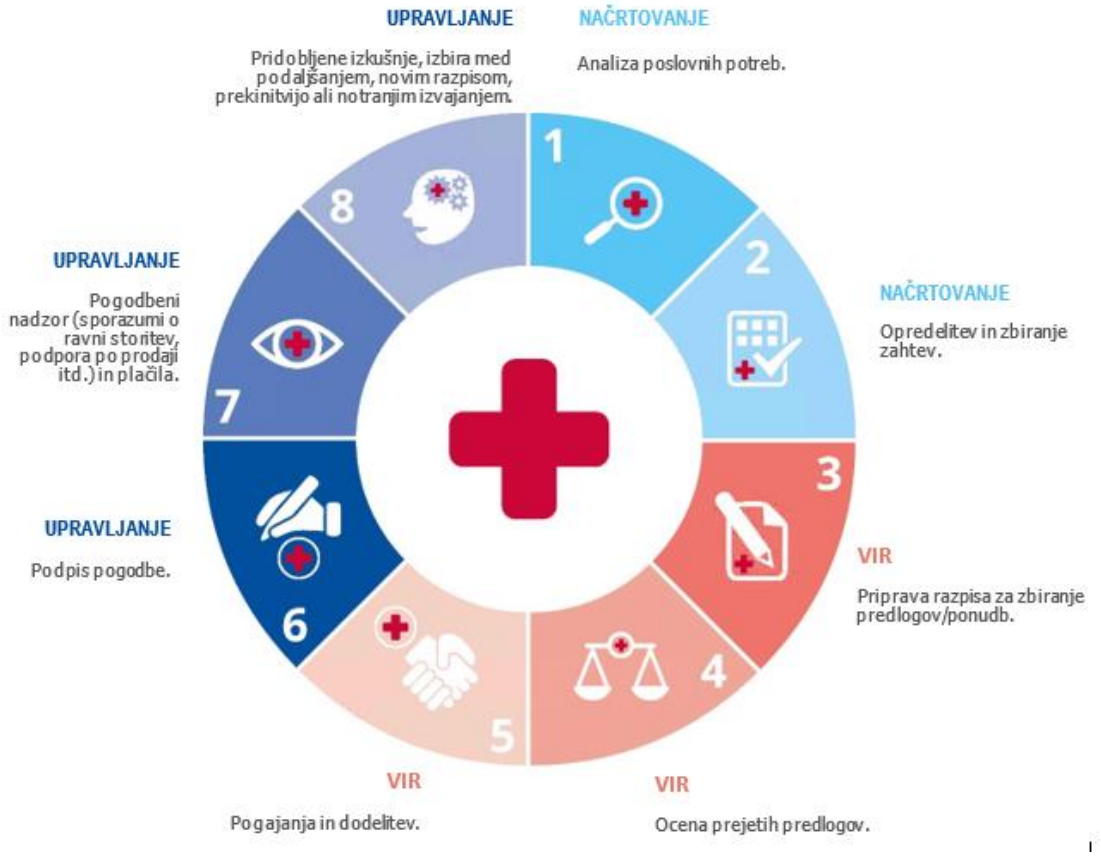
SMERNICE ZA JAVNO NAROČANJE V ZVEZI S KIBERNETSKO VARNOSTJO V BOLNIŠNICAH

Namen poročila je zagotoviti smernice zdravstvenim delavcem. Številne prakse in priporočila bodo koristili tudi drugim zdravstvenim organizacijam, saj so postopki javnega naročanja lahko zelo podobni. Poročilo je uporabno za zdravstvene delavce na tehničnih položajih v bolnišnicah, npr. vodilne delavce: informacijske (CIO) in tehnološke (CTO) direktorje, vodje informacijske varnosti (CISO), skupine informatikov ter uradnike za javna naročila v zdravstvenih organizacijah. V tem kratkem dokumentu so obravnavane ključne točke poročila – za več podrobnosti si oglejte publikacijo agencije ENISA: primere dobre prakse agencije ENISA za varnost zdravstvenih storitev, ki je bila objavljena februarja 2020.

POSTOPEK JAVNEGA NAROČANJA

Ker bolnišnični sistem sestavlja več komponent informacijske tehnologije, bi bilo treba kibernetsko varnost proučevati ločeno v vseh teh različnih komponentah. Kibernetska varnost bi morala biti del vseh različnih faz postopka javnega naročanja. V tem oddelku predstavljamo skupne faze postopka javnega naročanja za pridobitev proizvodov in storitev, vključno z medicinskimi pripomočki, informacijskimi sistemi in infrastrukturami.

Slika 1: Postopek javnega naročanja za bolnišnice po fazah



- Faza načrtovanja: bolnišnica najprej analizira svoje potrebe in zbere zahteve iz več notranjih oddelkov. V primeru pridobitve nove storitve v oblaku bi moral na primer tehnološki direktor opredeliti potrebe in razumeti, katere vrste uporabe bo ta storitev pokrivala.

- Faza vira: nato se zahteve pretvorijo v tehnične specifikacije, v sodelovanju z uradom za javna naročila pa se začne postopek javnega naročanja (npr. objavi se javni razpis). Bolnišnica prejme določene ponudbe, odbor (vključno s tehničnim direktorjem/vodjo informacijske varnosti in/ali članom skupine informatikov) oceni ponudbe in izbere najprimernejše proizvode. Z izvajalcem se izvedejo pogajanja, čemur sledi dodelitev naročila.

- Faza upravljanja: nazadnje je pogodba (upravljanje in spremljanje) dodeljena skrbniku v bolnišnici, ki je odgovoren za zaključek razpisa in prejemanje povratnih informacij o dejanski učinkovitosti opreme/sistema/storitve od uporabnikov.

VRSTE JAVNIH NAROČIL V BOLNIŠNICAH

Preglednica 1: Vrste javnih naročil (taksonomija sredstev)

Vrsta javnega naročila	Opis vrste
Klinični informacijski sistemi	Vključuje javna naročila katere koli vrste programske opreme za zdravstveno oskrbo.
Medicinski pripomočki	Vsaka strojna oprema, namenjena zdravljenju, nadzoru ali diagnosticiranju bolezni.
Omrežna oprema	Omrežni vodi (koaksialni, optični), vhodi, usmerjevalniki, stikala, požarni zidovi, omrežja VPN, sistem za preprečevanje vdorov, sistem za zaznavanje vdorov itd.
Sistemi oskrbe na daljavo	Funkcije ali naprave za zagotavljanje oskrbe zunaj bolnišničnega okolja, zlasti kar danes imenujemo „storitve bolnišnične oskrbe na domu“.
Mobilne odjemalske naprave	Vsa programska oprema, ki zagotavlja zdravstveno pomoč ali zbiranje zdravstvenih podatkov in ni neposredno povezana z bolnišničnim omrežjem; na primer aplikacije za medicino na daljavo.
Identifikacijski sistemi	Sistemi za edinstveno identifikacijo bolnikov ali zdravstvenih delavcev (biometrični skenerji, čitalniki kartic itd.) ter zagotavljanje identifikacije in/ali pooblastil za dostop do informacijskih sistemov.
Sistemi upravljanja stavb	Vse vrste zgradb, povezane z zdravstvenimi ustanovami.
Industrijski nadzorni sistemi	Sistemi, ki nadzorujejo vse fizične vidike zdravstvenih domov, kot so sistemi za regulacijo porabe energije, sistemi zaklepanja vrat, zaprti varnostni sistemi tokokrogov.
Strokovne storitve	Vse vrste storitev, oddanih v zunanje ali notranje izvajanje, ki jih zagotovijo strokovnjaki ali podjetja: zdravstvene storitve, prevozi, računovodstvo, inženirstvo, IT, pravne storitve, vzdrževanje, čiščenje, priprava in dostava hrane itd.
Storitve v oblaku.	Vsak komunikacijski ali informacijski sistem ali drug informacijski sistem, ki se ne izvaja v zdravstveni ustanovi ali v objektu podatkovnega centra pod popolnim nadzorom oddelka IT zdravstvenega doma.

TAKSONOMIJA NEVARNOSTI

Različne vrste javnih naročil so povezane z različnimi nevarnostmi za okolje IKT v bolnišnici. Skupaj z oddelkom za informacijsko tehnologijo, varnost ali tveganje si oglejte taksonomijo nevarnosti, predstavljeno v nadaljevanju, da bi ugotovili, katere nevarnosti so za vašo organizacijo najpomembnejše. To bi morala biti ena od nalog IT v bolnišnici, ne glede na možnosti javnega naročanja.

Preglednica 2: Vrste nevarnosti (taksonomija nevarnosti)

Nevarnost	Primeri
Naravni pojavi	Požari, poplave ali potresi
Prekinitve v dobavni verigi	Odpoved ponudnika storitev v oblaku, odpoved ponudnika omrežnih storitev, izpad napajanja, okvara pri proizvajalcu medicinskih pripomočkov/neodgovornost proizvajalca medicinskih pripomočkov.
Človeške napake	Napaka v konfiguraciji zdravstvenega sistema, odsotnost revizijskih dnevnikov, nepooblaščen nadzor dostopa/pomanjkanje postopkov, neskladnost (BYOD), napaka zdravstvenega delavca/bolnika.
Zlonamerna dejanja	Zlonamerna programska oprema (virus, izsiljevalsko programje, BYOD), ugrabitev (kraja procesorske zmogljivosti, ugrabitev medicinskega pripomočka), socialni inženiring (ribarjenje, nastavljanje vab, kloniranje pripomočkov), tatvina (podatkov, pripomočka), nedovoljeno spreminjanje medicinskih pripomočkov, skimming, zavrnitev storitve, napadi na spletu, napadi na spletne aplikacije, notranja grožnja, fizična manipulacija/poškodba, kraja identitete, kibernetsko vohunjenje, mehanske motnje komponent.
Izpadi sistema	Napake programske opreme, zastarela strojna oprema, okvara pripomočka, napaka omrežnih komponent, nezadostno vzdrževanje.

PRIMERI DOBRIH PRAKS NA PODROČJU KIBERNETSKE VARNOSTI PRI JAVNEM NAROČANJU

Seznam primerov dobrih praks, ki so navedeni spodaj, ni izčrpen, vendar je lahko v veliko pomoč zdravstvenemu delavcu – informatiku, ki je odgovoren za nakup opreme v bolnišnici. Sklop primerov dobrih praks je skupek vseh podatkov, ki so jih prispevali zdravstveni delavci, s katerimi so bili opravljeni razgovori. Bralec lahko seznam prilagodi glede na prednostne naloge svoje organizacije.

Dobra praksa 1 Vključitev oddelka IT v različne faze javnega naročanja, da se zagotovi upoštevanje strokovnega znanja na področju kibernetske varnosti.

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: vse.

Povezane nevarnosti: vse.

Dobra praksa 2 Opredelitev ranljivosti in izvedba procesa upravljanja, da bi zagotovili, da se vse ranljivosti upoštevajo že pred naročilom novih proizvodov ali storitev in da se vseskozi spremljajo ranljivosti obstoječih proizvodov/storitev.

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: klinični informacijski sistemi, medicinski pripomočki, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: vse.

Dobra praksa 3 Razvoj politike posodobitev strojne in programske opreme, da se uporabijo najnovejši popravki za vaš operacijski sistem in programsko opremo ter da je protivirusna programska oprema redno posodobljena.

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 4 Okrepitev varnostnega nadzora brezžičnih komunikacij, da se zagotovi omejen in strogo nadzorovan dostop do brezžičnih omrežij v bolnišnici.

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: medicinski pripomočki, mobilne odjemalske naprave, identifikacijski sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, človeške napake.

Dobra praksa 5 Vzpostavitev politike preskušanja, da se zagotovi testiranje prepustnosti vseh novih ali novo konfiguriranih proizvodov in da so popravni ukrepi skladni z delovnimi parametri dejanskega okolja.

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: klinični informacijski sistemi, medicinski pripomočki, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, sistem upravljanja stavb, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, izpadi sistema, človeške napake.

Dobra praksa 6 Vzpostavitev načrtov neprekinjenega poslovanja, da se zagotovi, da izpad sistema ne bo motil osnovnih bolnišničnih storitev in da je vloga dobavitelja jasno opredeljena.

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 7 Upoštevanje težav v zvezi z interoperabilnostjo za zagotovitev, da ni varnostnih vrzeli pri že obstoječih komponentah (obstoječa oprema IT).

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: klinični informacijski sistemi, medicinski pripomočki, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: izpadi sistema, človeške napake, zlonamerna dejanja.

Dobra praksa 8 Omogočiti testiranje vseh komponent, da se zagotovi njihovo pričakovano delovanje: preverjanje enostavnosti uporabe, preverjanje pravilnosti rezultatov pod obremenitvijo in preverjanje varnostnih pomanjkljivosti (politika v zvezi s šibkimi gesli, injiciranje SQL-stavkov).

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: klinični informacijski sistemi, medicinski pripomočki, oddaljene odjemalske naprave, identifikacijski sistemi, storitve v oblaku, industrijski nadzorni sistemi, sistem oskrbe na daljavo, sistem upravljanja stavb, mobilne odjemalske naprave.

Povezane nevarnosti: zlonamerna dejanja, človeške napake, izpadi sistema, prekinitve v dobavni verigi.

Dobra praksa 9 Omogočiti revizije in beleženje za sledenje napadalcem in za ugotovitev, koliko informacij je bilo izgubljenih/ukradenih v primeru zlorabe sistema.

Faze javnega naročanja: vse.

Povezane vrste javnih naročil: medicinski pripomočki, sistemi oskrbe na daljavo, mobilne odjemalske naprave, industrijski nadzorni sistemi.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 10 Šifriranje občutljivih osebnih podatkov med mirovanjem in v pretoku z opredelitvijo politike za sisteme, storitve ali pripomočke, ki obdelujejo posebne kategorije osebnih podatkov iz člena 9 Splošne uredbe o varstvu podatkov.

Faze javnega naročanja: vse

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 11 Izvedba ocene tveganja v okviru postopka javnega naročanja.

Faze javnega naročanja: načrtovanje.

Povezane vrste javnih naročil: vse.

Povezane nevarnosti: vse.

Dobra praksa 12 Predhodno načrtovanje zahtev glede omrežja, strojne opreme in licenc, da se ugotovi, ali je treba pred namestitvijo opraviti dodatne nadgradnje in/ali nakupe z namenom prilagoditve novemu sistemu.

Faze javnega naročanja: načrtovanje.

Povezane vrste javnih naročil: klinični informacijski sistemi, omrežna oprema, identifikacijski sistemi, industrijski nadzorni sistemi.

Povezane nevarnosti: prekinitve v dobavni verigi, izpadi sistema, naravni pojavi, človeške napake.

Dobra praksa 13 Opredeliti nevarnosti, povezane s proizvodi ali storitvami, ki so predmet javnega naročanja, in zagotoviti stalno ugotavljanje nevarnosti v celotnem postopku javnega naročanja.

Faze javnega naročanja: načrtovanje, upravljanje.

Povezane vrste javnih naročil: vse.

Povezane nevarnosti: vse.

Dobra praksa 14 Ločitev omrežja, da zagotovite izolacijo in/ali filtriranje omrežnega prometa z namenom omejitve in/ali preprečevanja dostopa med različnimi omrežnimi conami.

Faze javnega naročanja: načrtovanje, vir.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 15 Opredelitev zahtev omrežja, da se zagotovi interoperabilnost in preprečijo vrzeli po vzpostavitvi topologije omrežja in komponent.

Faze javnega naročanja: načrtovanje.

Povezane vrste javnih naročil: klinični informacijski sistemi, omrežna oprema, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku, sistemi oskrbe na daljavo, mobilne odjemalske naprave.

Povezane nevarnosti: prekinitve v dobavni verigi, izpadi sistema, naravni pojavi.

Dobra praksa 16 Določiti osnovne varnostne zahteve in jih pri izbiri dobaviteljev pretvoriti v merila za upravičenost.

Faze javnega naročanja: načrtovanje, vir.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 17 Priprava namenskega razpisa za zbiranje predlogov za javno naročanje storitev v oblaku, ki upošteva tudi zakonodajne in politične zahteve.

Faze javnega naročanja: načrtovanje, vir.

Povezane vrste javnih naročil: storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi.

Dobra praksa 18 Dati prednost javnemu naročanju sredstev, ki so certificirana na podlagi shem/standardov kibernetske varnosti.

Faze javnega naročanja: vir.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 19 Izvedba ocene učinka v zvezi z varstvom podatkov pri načrtovanju javnega naročanja novega sistema ali storitve.

Faze javnega naročanja: vir.

Povezane vrste javnih naročil: klinični informacijski sistemi, medicinski pripomočki, omrežna oprema, sistem oskrbe na daljavo, mobilni odjemalski pripomočki, identifikacijski sistemi, strokovne storitve, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, človeške napake.

Dobra praksa 20 Nastavitev vhodov, ki omogočajo nadaljnjo povezanost obstoječih sistemov/strojev, ter zagotovitev mejnega nadzora v primeru težav znotraj teh skupin.

Faze javnega naročanja: vir, upravljanje.

Povezane vrste javnih naročil: medicinski pripomočki, sistemi oskrbe na daljavo, mobilne odjemalske naprave, industrijski nadzorni sistemi.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 21 Zagotoviti usposabljanje na področju kibernetske varnosti o varnostnih praksah organizacije, da se zagotovi ustrezno usposabljanje notranjih uslužbencev ali zunanjih izvajalcev/svetovalcev, ki delajo na sedežu.

Faze javnega naročanja: vir, upravljanje.

Povezane vrste javnih naročil: vse.

Povezane nevarnosti: zlonamerna dejanja, človeške napake.

Dobra praksa 22 Oblikovanje načrtov za odzivanje ob izrednih dogodkih, ki zajemajo tudi novo pridobljene proizvode ali sisteme.

Faze javnega naročanja: vir, upravljanje.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 23 Vključitev prodajalca/proizvajalca v obvladovanje incidentov in opredelitev jasnih pogojev v razpisu za zbiranje predlogov.

Faze javnega naročanja: vir, upravljanje.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 24 Načrtovanje in spremljanje vzdrževalnih del za vso opremo, da se zagotovi ustrezna raven funkcionalnosti in odloči o kakršnih koli posodobitvah/popravkih itd.

Faze javnega naročanja: vir, upravljanje.

Povezane vrste javnih naročil: klinični informacijski sistemi, omrežna oprema, medicinski pripomočki, sistemi upravljanja stavb, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: človeška napaka, izpad sistema, naravni pojavi.

Dobra praksa 25 Oddaljeni dostop je treba čim bolj zmanjšati in ga urediti tako, da je zunanja komunikacija z dobaviteljem omejena samo na pripomoček, ki ga ta nadzira.

Faze javnega naročanja: vir, upravljanje.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, okvara dobavne verige, okvare sistema, človeške napake.

Dobra praksa 26 Zahtevati je treba popravke za vse komponente in vključiti informacije v razpis za zbiranje predlogov.

Faze javnega naročanja: vir, upravljanje.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.

Dobra praksa 27 Treba je povečati kibernetsko ozaveščenost zaposlenih ter s tem zagotoviti, da se zaveda tveganj, povezanih z novo pridobljenimi proizvodi ali storitvami.

Faze javnega naročanja: upravljanje.

Povezane vrste javnih naročil: vse.

Povezane nevarnosti: vse.

Dobra praksa 28 Izvedba popisa sredstev in upravljanja konfiguracij, da se zagotovijo ustrezno posodabljanje popisa vsakič, ko se v okolje IKT doda nova komponenta ali se odstrani iz njega, in osnovne varnostne konfiguracije komponent IKT, ki se ustrezno upravljajo.

Faze javnega naročanja: upravljanje.

Povezane vrste javnih naročil: klinični informacijski sistemi, medicinski pripomočki, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi.

Povezane nevarnosti: zlonamerna dejanja, človeške napake, izpadi sistema.

Dobra praksa 29 Vzpostavitev namenskih nadzornih mehanizmov za dostop do medicinskih pripomočkov, ki morajo biti zaščiteni tudi fizično in dostopni samo strokovnemu osebju.

Faze javnega naročanja: upravljanje.

Povezane vrste javnih naročil: medicinski pripomočki, sistem upravljanja stavb, identifikacijski sistemi.

Povezane nevarnosti: zlonamerna dejanja, človeške napake.

Dobra praksa 30 Načrtovanje pogostega testiranja prepustnosti ali po vsaki spremembi zgradbe/sistema in vključitev pogojev v razpis za zbiranje predlogov.

Faze javnega naročanja: vir, upravljanje.

Povezane vrste javnih naročil: medicinski pripomočki, klinični informacijski sistemi, omrežna oprema, sistem oskrbe na daljavo, mobilne odjemalske naprave, identifikacijski sistemi, industrijski nadzorni sistemi, storitve v oblaku.

Povezane nevarnosti: zlonamerna dejanja, prekinitve v dobavni verigi, izpadi sistema.