Splošna bolnišnica
Novo mesto

Politika upravljanja kakovosti in varnosti storitev tretjih strank

Odgovorna oseba za izvajanje politike:

Vodja tehnično-vzdrževalne službe
Vodja službe za varstvo pri delu in varstvo pred požarom
Vodja službe za informatiko
Vodja službe za investicije

Verzija: 1

Velja od: 3. 11. 2017

TERMINOLOŠKI SLOVAR

- Analiza tveganja - sistematična uporaba informacij za prepoznavanje virov in ocenjevanje tveganja
- Overitev - potrditev istovetnosti
- Enolični identifikator - sredstvo razpoznave točno določene osebe
- Grožnja - nekaj, kar ima potencial za povzročitev škode
- Informacija - iz podatkov v postopku obdelave dobimo informacijo
- Informacijski sistem - je urejen in organiziran sistem, ki uporabnike oskrbuje z vsemi potrebnimi informacijami za odločanje
- Mrežni servisi – servisi, ki delujejo v omrežju
- Mrežni viri – sredstva, ki so na voljo v omrežju
- Neprekinjenost storitev – storitve, ki delujejo glede na poslovne potrebe brez neželenih prekinitev
- Revizijski pregled – pregled aktivnosti nad informacijskim sistemom
- Segment - zaključena celota na omrežnem (L3) sloju (Broadcast domena)
- Sistemski skrbnik - skrbnik posameznega informacijskega sistema
- Tretje stranke - partnerji ali pogodbeni sodelavci, ki izvajajo storitve za organizacijo izvajalca zdravstvene dejavnosti
- Varnostna politika - pravila za zagotavljanje postopkov informacijske varnosti

Povezava na Vzorčna notranja pravila za zajem in hrambo gradiva v digitalni obliki: Priloga 25

1. POLITIKA UPRAVLJANJA KAKOVOSTI IN VARNOSTI STORITEV TRETJIH STRANK

1.1 Namen

Izvajalec zdravstvene dejavnosti je odgovoren za zagotavljanje ravni storitev, ki jih izvaja tretja stranka, zato mora imeti zadosten nadzor in vpogled v izvajanje storitev tretje stranke. Okvir za naročanje storitev pri tretjih strankah predstavljajo veljavna zakonodaja in interni akti izvajalca zdravstvene dejavnosti.

Dokument predstavlja okvir za upravljanje kakovosti storitev tretjih strank. Namen dokumenta je opredeliti postopke, s katerimi organizacija zagotovi, da tretje stranke izvajajo dogovorjeno raven storitev in zagotavljajo ustrezno varnost informacij.

1.2 Pogodbeno urejanje razmerij s tretjimi strankami

Pogodba o izvajanju storitev, ki jo izvaja tretja stranka, opredeljuje opis storitev in predvideni rok trajanja oziroma dobo opravljanja teh storitev. Pri opisu storitev so opredeljeni cilji in vnaprej določene ravni izvajanja storitev, vključno z opredelitvijo preverljivih kriterijev za doseganje teh ravni, načinom poročanja ter pravico nadzorovanja pogodbenih obveznosti, lahko tudi s strani tretjih strank.

Določila o seznanjenosti in sprejemanju varnostnih zahtev za tretje stranke, ki jih določajo varnostne politike izvajalca zdravstvene dejavnosti, se vključi v pogodbo ali doda kot samostojno prilogo.

Določila tretje stranke obvezujejo, da:

- osebnih, občutljivih osebnih in internih informacij ne bodo posredovali drugim osebam;
- jih bodo varovali tako, da bo preprečeno nepooblaščeno razkritje;
- jih ne bodo uporabljali na kakršenkoli način, izven načina, dogovorjenega s pogodbo.

Pri tem se skladno s pogodbo izvaja varovanje skozi celotno obdobje sodelovanja in pa določeno obdobje po zaključku sodelovanja s tretjo stranko.

V pogodbo s tretjo stranko se vključi določbe, ki se nanašajo na:

- način poročanja ter obveščanja o varnostnih incidentih**,**
- postopke za zaščito sredstev za izvajanje storitev,
- zahteve glede varovanja podatkov izvajalca zdravstvene dejavnosti,
- nadzor dostopa, vključno z dovoljenimi metodami dostopa tretje stranke,
- vodenje in dostopnost seznama izvajalcev, pooblaščenih za izvajanje storitev,
- obveznosti glede namestitve in vzdrževanja strojne in programske opreme tretje stranke ter zahtevanih fizičnih in logičnih nadzornih mehanizmov dostopa do sistemov, storitev in informacij,

- zahteve, da tretja stranka omrežje varuje pred grožnjami iz zunanjih omrežij z opremo, ki zagotavlja največjo možno varnost pred zlonamerno programsko opremo in zunanjimi vdori do sistemov, storitev in podatkov,
- zahteve, da bo izvajalcu zdravstvene dejavnosti na pisno zahtevo posredoval vse podatke, ki so v zvezi z zagotovitvijo varnosti sistemov, storitev in informacij za izvajanje storitev,
- pravico do revizijskega pregleda (izvajalec zdravstvene dejavnosti si pridržuje pravico do preverjanja ravni varnosti, ki ga zagotavlja tretja stranka, z varnostnimi pregledi informacijskega sistema tretje stranke),
- možnost vključitve podizvajalcev,
- načine zagotavljanja, da se vse osebe, ki so povezane z zunanjim izvajanjem storitev, vključno s podizvajalci, zavedajo svojih obveznosti glede zagotavljanja ustrezne varnosti.

V pogodbo se vključi tudi določbe, ki določajo ukrepe v primeru kršitev obveznosti iz pogodbe in odgovornost pogodbenih strank oziroma sankcije.

Kjer je potrebno, se izvajalec zdravstvene dejavnosti pri naročanju storitev pri tretji stranki dogovori o neprekinjenosti storitev, ki se morajo ohraniti tudi v primeru nepredvidenih dogodkov, npr. pri večjih okvarah ali nesrečah.

Pred sklenitvijo pogodbe mora osebje tretje stranke, ki bo izvajalo dela po pogodbi, podpisati izjavo o seznanitvi in sprejemanju varnostnih zahtev, ki jih določa varnostna politika izvajalca zdravstvene dejavnosti.

1.3 Upravljanje sprememb pogodbenih storitev tretjih strank

Spremembe v zvezi z zagotavljanjem pogodbenih storitev se upravlja tako, da skrbnik pogodbe najmanj enkrat letno preverja postopke tretje stranke. Skrbnik pogodbe je odgovoren za:

- informiranje tretje stranke o relevantnih določbah varnostne politike izvajalca zdravstvene dejavnosti,
- nadzor in spremljanje ravni izvajanja storitev in varovanja informacij tretje stranke,
- pregledovanje poročil in zapisov tretje stranke,
- spremljanje sprememb pri izvajanju storitev in po potrebi sprožitev postopka za spremembo postopkov oziroma dokumentov varnostne politike in revizijo pogodbe s tretjo stranko.

1.4 Politika nadzora dostopa tretjih strank do informacijskega sistema in informacij

Ko se pojavi potreba po dostopu tretjih strank do informacij ali informacijskega sistema izvajalca zdravstvene dejavnosti, se najprej izvede analizo tveganja in ugotovi potrebne varnostne ukrepe. Dostop tretjim strankam do informacij in informacijskega sistema ni dovoljen, dokler niso

implementirani ustrezni varnostni in nadzorni mehanizmi in niso stopila v veljavo potrebna interna pravila in pogodba, ki definira pogoje dostopa.

Pravila za določanje dostopov opisujejo načine dostopa in omogočajo nadzor nad dostopi do informacij in informacijskega sistema. Pravila morajo vedno odražati poslovne potrebe izvajalca zdravstvene dejavnosti in s tem povezane varnostne zahteve. Osnova za izdelavo pravil je varnostna razvrstitev podatkov, ki jo določa Politika o navodilih za klasifikacijo, označevanje in ravnanje z informacijami.

Pravila za določanje dostopov se morajo stalno prilagajati spremembam v razvrstitvi, poslovnih procesih in informacijskem sistemu.

Tretjim strankam omogočimo dostop do samo tistih informacij in sistemov, ki jih nujno potrebujejo pri svojem delu. Na ta način preprečujemo nepooblaščen dostop.

Tretje stranke pred začetkom dela seznanimo z varnostnimi politikami, ki jih je tretja stranka dolžna upoštevati. Pogoji sodelovanja in ukrepi nadzora so zapisani v pogodbi med tretjo stranko in izvajalcem zdravstvene dejavnosti. S podpisom pogodbe se tretja stranka obveže spoštovati in upoštevati varnostne predpise in varovati vse podatke, do katerih imajo dostop.

1.4.1 Logični dostop do informacijskega sistema in informacij

Za odobritev in izvedbo postopka za dostop v omrežje za tretje stranke je potrebno pripraviti zahtevek ali izdelati drug dokument, ki vsebuje vse predpisane podatke. Zahtevek za zunanjega sodelavca izpolni vodja organizacijske enote, v kateri je tak dostop potreben. Zahtevek, ki vsebuje vse predpisane podatke za oddaljen dostop je v prilogi varnostne politike z naslovom Priloga 29_Zahtevek zunanje stranke za oddaljen dostop do omrežja SB NM.

Za tretje stranke se pripravi poseben izoliran segment omrežja, kamor se lahko priključijo. Od tam imajo omejen (filtriran) dostop preko požarne pregrade do omrežja izvajalca zdravstvene dejavnosti, in sicer samo s servisi, ki so potrebni in odobreni za njihovo delo in samo do notranjih mrežnih virov, ki so specificirani v odobrenem zahtevku in potrebni za njihovo delo.

Tretje stranke se pri vstopu v omrežje izvajalca zdravstvene dejavnosti overijo z uporabniškim imenom in geslom. Vsi dostopi tretjih strank do informacijskega sistema se beležijo ves čas sodelovanja s tretjo stranko in pregledujejo enkrat mesečno.

- Vodja organizacijske enote, ki potrebuje dostop za tretje stranke, izpolni zahtevek. V zahtevku pa navede:
    - osebne podatke kontaktne osebe tretje stranke (ime, priimek, telefonska številka),
    - morebitne časovne omejitve dostopa,
    - način dostopa,
    - namen oddaljenega dostopa (do katerih mrežnih virov in mrežne opreme potrebuje dostop),
    - tehnične podatke (IP številka).

- Odgovorna oseba za informacijski sistem pregleda zahtevek in dopolni parametre obrazca.
- Priporočljivo je, da se za dostop tretjih strank glede na ocenjeno stopnjo tveganja pripravijo ločeni segmenti omrežja, ki so povezani z omrežjem izvajalca zdravstvene dejavnosti preko požarne pregrade.
- Tretji stranki se omogoči dostop le do tistih servisov, ki so potrebni za delo tretje stranke – v skladu z odobrenim zahtevkom.
- Določi se gesla za dostop do notranjih mrežnih virov za tretjo stranko – v skladu z odobrenim zahtevkom.
- Sistemski skrbnik izvajalca zdravstvene dejavnosti izvede test dostopa.
- Tretja stranka podpiše zahtevek za dostop in s tem potrdi prevzem gesel ter seznanjenost z varnostnimi pravili dostopa.
- Zahtevek se arhivira na ustrezno mesto.

Tretjim strankam se prekine dostop v omrežje takoj, ko dostopa do informacijskega sistema izvajalca zdravstvene dejavnosti ne potrebujejo več oziroma najpozneje, ko preneha pogodbeno razmerje med izvajalcem zdravstvene dejavnosti in tretjo stranko.

Čas prekinitve dostopa za tretjo stranko sporoči sistemskim skrbnikom vodja organizacijske enote, ki je odobril dostop. Če je že vnaprej znano, da bo dostop omogočen za določeno dobo, se predviden datum prekinitve dostopa napiše že na zahtevo.

Dostop v omrežje se prekine v primeru kršitve določil varnostnih predpisov in navodil.

Če se pojavi sum kršitve varnostnih predpisov in navodil, se dostop v omrežje začasno onemogoči, dokler se ne ugotovi dejanskega stanja kršitve.

1.4.2 Fizični dostop do sistemov

Obiskovalci ne smejo vstopati in se gibati nenadzorovano po območjih upravnih in zdravstvenih pisarn, opredeljenih v Politiki fizične zaščite in fizičnega dostopa, pač pa le v spremstvu nekoga od zaposlenih, ki ima pravico dostopa v te prostore.

Vzdrževanje opreme lahko izvajajo le pooblaščene tretje stranke, s katerimi je sklenjena pogodba z ustreznimi členi glede varovanja informacij. Dostop tretje stranke do strojne opreme je vedno nadziran. Vzdrževalna dela se izvajajo na mestu, kjer se oprema nahaja. Če to ni mogoče, se odstrani nosilec podatkov iz opreme in se ga varno shrani. Če podatkov ni mogoče odstraniti ali kako drugače zaščititi, mora biti postopek vzdrževanja nadzorovan.