Splošna bolnišnica
Novo mesto

Politika fizične zaščite in fizičnega dostopa

Odgovorne osebe za izvajanje politike:

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

Verzija: 1

Velja od: 3. 11. 2017

TERMINOLOŠKI SLOVAR

- Vstopna točka – točka dostopa do informacijskega sistema
- Samodejno zaklepanje – avtomatizirano zaklepanje računalniške opreme

Povezava na Vzorčna notranja pravila za zajem in hrambo gradiva v digitalni obliki: Priloga 14

1. POLITIKA NADZORA DOSTOPA DO APLIKACIJ, INFORMACIJ IN SISTEMOV

1.1 Namen

Politika fizične zaščite in fizičnega dostopa določa pravila in postopke fizičnih dostopov do informacijskega sistema. Pravila in postopki omogočajo dostop do informacijskega sistema za pooblaščene osebe. Nepooblaščen dostop ima lahko za posledico razkritje podatkov izvajalca zdravstvene dejavnosti, med katere spadajo osebni podatki in občutljivi osebni podatki ter podatki, ki so klasificirani samo za interno rabo.

Pravila in postopki fizične zaščite in fizičnega dostopa morajo biti usklajeni z varnostnimi zahtevami in hkrati omogočati neovirano izvajanje zdravstvenih storitev. Določitev pravil temelji na razvrstitvi informacij, zakonodaji in pogodbenih obveznostih, ki zadevajo zaščito dostopov do informacij in storitev. Politiko fizične zaščite in fizičnega dostopa je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

1.2 Fizični dostop do varovanih območij

Varovanje posameznih prostorov se razlikuje po tem, v kakšno območje spadajo. Pri tem se ne sme ovirati delovanja izvajalca zdravstvene dejavnosti.

1.2.1 Območje javnega dostopa (čakalnice, hodniki, bolniške sobe itd.)

Območje javnega dostopa ni posebej varovano, zato se v tem področju ne sme hraniti in obdelovati osebnih podatkov ali občutljivih osebnih podatkov ter podatkov, ki so klasificirani samo za interno rabo. Izvajalec zdravstvene dejavnosti mora te prostore organizacije nadzorovati, da se obiskovalci nahajajo tam samo v delovnem času izvajalca zdravstvene dejavnosti in za namene uporabe storitev, obiska oziroma zaradi pogodbenih obveznosti.

1.2.2 Območje zdravstvenih pisarn (zdravniške pisarne, pisarne medicinskih sester itd.)

Območje zdravstvenih pisarn je namenjeno hrambi in obdelavi osebnih podatkov ali občutljivih osebnih podatkov. Izvajalec zdravstvene dejavnosti mora zagotavljati primerno varovanje, da ne more prihajati do nepooblaščenega dostopa v to območje. Dostop mora biti urejen s kontrolo dostopa (ključ, brezkontaktna kartica ipd.). Prostori, kjer se hranijo osebni podatki ali občutljivi osebni podatki morajo biti izven delovnega časa nadzorovani z načini tehničnega varovanja (kontrola vstopnih točk s protivlomnim alarmom, varnostno službo itd.).

1.2.3 Območje upravnih pisarn (pisarne vodstva, finančne službe, splošnih služb itd.)

Območje upravnih pisarn je namenjeno hrambi in obdelavi osebnih podatkov ali občutljivih osebnih podatkov ter podatkov, ki so klasificirani samo za interno rabo. Izvajalec zdravstvene dejavnosti mora zagotavljati primerno varovanje, da ne more prihajati do nepooblaščenega dostopa v to območje. Dostop mora biti urejen s kontrolo dostopa (ključ, brezkontaktna kartica ipd.). Prostori, kjer se hranijo osebni podatki ali občutljivi osebni podatki ter podatki, ki so klasificirani samo za interno rabo, morajo biti izven delovnega časa nadzorovani z načini tehničnega varovanja (kontrola vstopnih točk s protivlomnim alarmom, varnostno službo itd.).

1.2.4 Območje računalniškega IS (podatkovni center itd.)

Območje računalniškega IS je namenjeno hrambi in obdelavi osebnih podatkov ali občutljivih osebnih podatkov ter podatkov, ki so klasificirani samo za interno rabo. Izvajalec zdravstvene dejavnosti mora zagotavljati primerno varovanje, da ne more prihajati do nepooblaščenega dostopa v to območje. Dostop mora biti urejen s kontrolo dostopa (ključ, brezkontaktna kartica, video varovanje itd.), ki beleži dostope posameznikov do območja. Fizični dostopi v strežniški prostor se evidentirajo na vpisni list, ki je v strežniškem prostoru nameščen na vidnem mestu. Primer vpisnega lista je v dokumentu Evidenca dostopa do strežniškega prostora. Vrata v prostore morajo biti opremljena s slepo ključko (možen dostop samo z izbranim sredstvom kontrole dostopa) in mehanizmom za samozapiranje. Prostori, kjer se hranijo osebni podatki ali občutljivi osebni podatki ter podatki, ki so klasificirani samo za interno rabo, morajo biti izven delovnega časa nadzorovani z načini tehničnega varovanja (kontrola vstopnih točk s protivlomnim alarmom, varnostno službo itd.).

1.2.5 Območje komunikacijskega sistema (komunikacijske omare, komunikacijski vodi itd.)

Območje komunikacijskega sistema je namenjeno prenosu komunikacij. Izvajalec zdravstvene dejavnosti mora zagotavljati primerno varovanje, da je območje zaščiteno pred prestrezanjem komunikacij. Območje komunikacijskega prostora je lahko razdeljeno in obsega lastne prostore ali omare, ki morajo biti ustrezno varovane oz. opremljene s ključavnicami in zaklenjene.

Komunikacijski kabli, po katerih se prenašajo podatki, morajo biti zaščiteni pred prestrezanjem ali poškodbami. Nameščajo se v ustrezne kanale. Ožičenje ne sme predstavljati ovir pri gibanju. Vsi mrežni priključki, ki niso v uporabi, morajo biti neaktivni.

1.3 Politika čiste mize

Zaposleni ne smejo puščati nosilcev podatkov (fizični izvodi, elektronski izvodi) z osebnimi podatki ali občutljivimi osebnimi podatki ter podatki, ki so klasificirani samo za interno rabo, na pisarniških mizah ali drugih mestih, kjer so dostopni nepooblaščenim osebam. Nosilce podatkov morajo uporabniki varno shraniti po končanem delovnem času oziroma ko dlje časa niso fizično prisotni v prostoru. Izven delovnega časa mora biti vsa pisarniška oprema, kjer se hranijo nosilci podatkov z osebnimi podatki ali občutljivimi osebnimi podatki ter podatki, ki so klasificirani samo za interno rabo, zaklenjena ali drugače varovana, računalniška oprema pa fizično in programsko varovana.

1.4 Politika praznega zaslona

Nepooblaščenim osebam mora biti onemogočen vpogled na računalniške zaslone . Vpogled lahko v posameznih primerih dovolijo zaposleni, če gre za obdelavo podatkov o uporabniku storitev, ki mora imeti vpogled v svoje osebne podatke ali občutljive osebne podatke.

Ob odhodu s svojega delovnega mesta morajo zaposleni vključiti ohranjevalnik zaslona in zakleniti računalnik. Po 20 minutah nedejavnosti zaposlenega se avtomatično vključi ohranjevalnik zaslona, računalnik pa se samodejne zaklene. Ob koncu delovnega časa se mora zaposleni odjaviti iz sistema.

1.5 Odstranjevanje podatkov

Vsi nosilci podatkov z osebnimi podatki ali občutljivimi osebnimi podatki ter podatki, ki so klasificirani samo za interno rabo, se morajo uničiti na način, ki onemogoči branje vseh ali dela uničenih podatkov. Zaposleni nosilcev podatkov ne smejo odmetavati v koše za smeti. Za odstranitev podatkov se mora pripraviti primerne mehanizme (uničevanje, komisijski zapisnik o uničenju ipd.), ki zagotavljajo, da ne more priti do zlorabe podatkov.

1.6 Politika proti zlorabi opreme računalniškega informacijskega sistema

V organizaciji se vzdržuje popis sredstev opreme računalniškega informacijskega sistema. Vsaka predaja ali sprejem opreme morata biti zabeležena. Izvajalec zdravstvene dejavnosti mora izvajati ukrepe za preprečevanje kraje opreme. Vsa oprema ima identifikacijske oznake. Popis sredstev se preverja najmanj 1-krat letno. Za premeščanje računalniške opreme je zadolžena pooblaščena oseba, ki vodi evidenco o opremi računalniškega informacijskega sistema in beleži spremembe v računalniškem informacijskem sistemu.

1.7 Beleženje dostopov brezkontaktne kartice ali daljinca

Sistem kontrole dostopa po posameznih kontrolerjih beleži vse dogodke za obdobje 3 let, razen pri lekarniškem sistemu, ki je lokalen in ne omogoča spremljanje zgodovine dogodkov. Vpogled v dogodke lahko opravi pooblaščena oseba in je dovoljen samo v primeru incidenta ali preverjanja pravilnosti delovanja sistema. Podatki se hranijo v lokalni bazi JantarV7 na računalniku, nameščenem v strežniški sobi.