ZD Radlje ob Dravi

Krovna politika varovanja informacij

KAZALO VSEBINE

1 KROVNA POLITIKA VAROVANJA INFORMACIJ

1.1 TERMINOLOŠKI SLOVAR

- **Grožnja** - je nekaj, kar ima potencial za povzročitev škode
- **Informacijske in komunikacijske tehnologije** - se nanaša na izdelke in prakse, ki se uporabljajo za shranjevanje, zapisovanje in druge vrste obdelav informacij
- **Izvajalec zdravstvene dejavnosti** - zdravstvene organizacije
- **Načrt za obravnavo tveganj** - nabor ocenjenih ukrepov z določenimi odgovornimi osebami in datumi izvedbe
- **Notranja presoja** - presoja, ki jo izvedejo izvajalci zdravstvene dejavnosti v svoji organizaciji
- **Ocena tveganj** - celoten proces analize tveganja in vrednotenja tveganja
- **Politika varovanja informacij** - pravila za zagotavljanje postopkov informacijske varnosti
- **Sistem za upravljanje varovanja informacij (SUVI)** - sistem, ki temelji na pristopu do poslovnega tveganja, ki zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varovanja informacij
- **Standardi informacijske varnosti** - priznani dokumenti, ki predpisujejo dobre prakse varovanja informacij
- **Tekstovni in slikovni izpisi** - pisna in slikovna dokumentacija
- **Varnostna kršitev** - ravnanje, ki je v neskladju z varnostnimi politikami
- **Varnostni incident** - eden ali serija neželenih ali nepričakovanih dogodkov v zvezi z varovanjem informacij, za katere je zelo verjetno, da bodo ogrozili poslovanje in varovanje informacij
- **Varnostni ukrep** - kontrola, ki zagotavlja izboljšanje varovanja informacij
- **Vodstveni pregled** - pregled stanja informacijske varnosti najvišjega vodstva organizacije
- **Zunanje in notranje grožnje** - grožnje, ki prihajajo iz okolja in same organizacije

1.2 NAMEN POLITIKE VAROVANJA INFORMACIJ

Zdravstveni dom se zaveda vrednosti informacij izvajalcev zdravstvene dejavnosti, ki bodo vključeni v splošno uporabo informacijskih in komunikacijskih tehnologij pri preprečevanju, diagnosticiranju, zdravljenju in spremljanju bolezni ter pri odločanju o zdravju in načinu življenja (v nadaljnjem besedilu: eZdravje). Za uspešno zagotavljanje zdravstvene dejavnosti so varne in zanesljive informacije ključnega pomena. Z upoštevanjem določil veljavne zakonodaje ter priporočil standardov informacijske varnosti je vzpostavljen sistem za upravljanje varovanja informacij (v nadaljnjem besedilu: SUVI), ki zagotavlja vzpostavitev, vpeljavo, delovanje, spremljanje, pregledovanje, vzdrževanje in izboljševanje varovanja informacij. S politiko varovanja informacij vodstvo izraža svojo odgovornost in zavezanost k zagotavljanju ustrezne varnosti informacijskega premoženja. Zaposleni in pogodbeni sodelavci izvajalcev zdravstvene dejavnosti ter vsi ostali uporabniki informacij na področju eZdravja pa potrjujejo svojo odgovornost glede izvajanja politike varovanja informacij.

Cilj varovanja informacij je stalno izboljševanje kakovosti varnega upravljanja z informacijami ter preprečevanje oziroma zmanjšanje posledic varnostnih incidentov na najmanjšo možno mero. Namen politike varovanja informacij je določiti pomembnost informacij za ustrezno delovanje storitev izvajalcev zdravstvene dejavnosti na področju eZdravja in jih ustrezno zaščititi v smislu zagotavljanja:

- **zaupnosti:** zagotoviti dostop do informacij samo pooblaščenim osebam
- **celovitosti**: varovanje točnosti in popolnosti informacij s preprečevanjem nepooblaščenih sprememb
- **razpoložljivosti**: zagotavljanje pooblaščenim osebam dostop do informacij, ko jih potrebujejo

Politika varovanja informacij določa varnostne ukrepe in postopke v skladu z varnostno občutljivostjo, poslovno vrednostjo in kritičnostjo informacij ne glede na obliko, v kateri se informacije pojavljajo: v elektronski obliki na računalnikih, prenosnih pomnilniških medijih ter pri prenosu preko omrežja ali v fizični obliki na tekstovnih ter slikovnih izpisih oziroma pri ustnem posredovanju.

Zaradi vse večje odvisnosti poslovanja od informacijskih in komunikacijskih tehnologij se povečuje ranljivost za različne zunanje in notranje grožnje, ki postajajo čedalje bolj razširjene in učinkovite pri povzročanju škode. Politika varovanja informacij s pomočjo varnostnih kontrol postavlja celovit okvir za zagotavljanje varovanja informacij na področju eZdravja ter izpolnjevanja zahtev zakonodaje.

Politika varovanja informacij ter navodila in postopki varovanja informacij so razviti in usklajeni z zahtevami veljavne zakonodaje in priporočili standardov informacijske varnosti
ISO/IEC 27001 in ISO/IEC 27002.

1.3 OBSEG POLITIKE VAROVANJA INFORMACIJ

SUVI mora obsegati celoten informacijski sistem izvajalca zdravstvene dejavnosti, politika varovanja informacij pa mora biti skladna z zahtevami Ministrstva za zdravje. S sprejeto politiko in navodili glede varovanja informacij izvajalec zdravstvene dejavnosti potrjuje svojo odgovornost glede izvajanja določil SUVI.

SUVI vključuje vse vidike varovanja informacij, ki so predstavljeni v naslednjih poglavjih:

1.3.1 Politika varovanja informacij

dokument o politiki varovanja informacij, pregledovanje in upravljanje politike varovanja informacij

1.3.2 Organiziranost varovanja

obvladovanje varovanja informacij pri izvajalcih zdravstvene dejavnosti in dostopa tretjih strank do informacij

1.3.3 Upravljanje s sredstvi
opredelitev lastnikov informacijskih sredstev, odgovornosti za varnostne ukrepe, varnostna razvrstitev informacij

1.3.4 Varovanje v zvezi z osebjem
ustrezno preverjanje kandidatov za zaposlitev, izjava o zaupnosti, usposabljanje uporabnikov za varnostne postopke in pravilno uporabo sredstev informacijske tehnologije, postopki pri prenehanju delovnih razmerij zaposlenih

1.3.5 Fizično in okoljsko varovanje
fizična zaščita varovanih območij pred nepooblaščenim dostopom, škodo in motnjami, fizična zaščita informacijske opreme ter tehnične infrastrukture

1.3.6 Upravljanje s komunikacijami in obratovanjem
vzpostavitev odgovornosti in postopkov za obratovanje računalniškega informacijskega sistema, načrtovanje in priprava za zagotovitev primernih zmogljivosti računalniškega informacijskega sistema, zaščita pred zlonamerno programsko opremo, izdelava rezervnih kopij podatkov, varovanje v računalniških omrežjih, ravnanje z nosilci podatkov, obvladovanje izmenjave podatkov med organizacijami, nadzor informacijskih sistemov in beleženje dogodkov in incidentov

1.3.7 Obvladovanje dostopa do informacijskega sistema
kontrola dodeljevanja pravice dostopa do informacijskih sistemov in storitev, odgovornosti uporabnikov, kontrola dostopa do operacijskega sistema, kontrola dostopa do aplikacij in informacij, obvladovanje uporabe prenosne opreme in dela na daljavo

1.3.8 Nabava, razvoj in vzdrževanje informacijskega sistema
opredelitev varnostnih zahtev informacijskih sistemov, varnostne kontrole v aplikacijah, uporaba šifriranja podatkov, ravnanje z dostopom do sistemskih datotek

1.3.9 Upravljanje z varnostnimi incidenti
poročanje o varnostnih incidentih, odgovornosti in postopki ravnanja z varnostnimi incidenti

1.3.10 Upravljanje neprekinjenega poslovanja
razvoj in vzdrževanje ustreznih načrtov za hitro ponovno vzpostavljanje storitev pri izvajalcih zdravstvene dejavnosti

1.3.11 Usklajenost
usklajenost z zakonskimi zahtevami, usklajenost s politiko varovanja informacij

1.4 SPLOŠNA ODGOVORNOST IN ODGOVORNOST ZA POSAMEZNA PODROČJA VAROVANJA INFORMACIJ

1.4.1 Center za informatiko v zdravstvu (CIZ)

Center za informatiko v zdravstvu (v nadaljnjem besedilu: CIZ (vse njegove naloge v prehodnem obdobju opravlja Ministrstvo za zdravje)) je odgovoren za preverjanje vzpostavitve SUVI, za spremljanje in nadziranje učinkovitosti varnostnih ukrepov in postopkov. CIZ določi pooblaščene osebe, ki bodo izvajale naloge:

- pripravе dokumentov politik varovanja informacij ter postopkov in navodil za izvajalce zdravstvene dejavnosti za področje eZdravja
- priprave navodil in postopkov za izvajanja ocene tveganj
- najmanj enkrat letno izvedbe ocene tveganj
- najmanj enkrat letno priprave poročil, ki sledi ugotovitvam ocene tveganj
- priprave načrta za obravnavo tveganj
- zagotavljanja ozaveščenosti izvajalcev zdravstvene dejavnosti glede varovanja informacij ter ustrezne usposobljenosti za izvajanje politike varovanja informacij ter postopkov in navodil za varovanje informacij
- komuniciranja z izvajalci zdravstvene dejavnosti o dolžnostih, ki jih zadevajo v SUVI
- upravljanja z varnostnimi incidenti in varnostnimi pomanjkljivostmi
- izvedbe varnostnih ukrepov za izboljšanje stanja varovanja informacij

1.5 IZVAJALCI ZDRAVSTVENE DEJAVNOSTI

Za upoštevanje politik varovanja informacij in izvajanje posameznih varnostnih ukrepov in postopkov so zadolženi vsi izvajalci zdravstvene dejavnosti, ki se vključujejo v eZdravje. Naloge izvajalcev zdravstvene dejavnosti so:

- izvajanje politike varovanja informacij ter postopkov in navodil za varovanje informacij
- najmanj enkrat letno izvesti notranjo presojo in pripraviti zapisnik notranje presoje
- najmanj enkrat letno izvesti vodstveni pregled in pripraviti zapisnik vodstvenega pregleda ter ga posredovati CIZ
- zagotavljanje ozaveščenosti zaposlenih glede varovanja informacij ter ustrezne usposobljenosti za izvajanje politike varovanja informacij ter postopkov in navodil za varovanje informacij
- komuniciranje z zunanjimi sodelavci o dolžnostih, ki jih zadevajo v SUVI
- upravljanje z varnostnimi incidenti in varnostnimi pomanjkljivostmi in poročanje CIZ
- izvedba varnostnih ukrepov za izboljšanje stanja varovanja informacij in poročanje CIZ

1.6 POSEBNE ODGOVORNOSTI IZVAJALCEV ZDRAVSTVENE DEJAVNOSTI

1.6.1 Poročanje incidentov in varnostnih pomanjkljivosti

V proces stalnega izboljševanja nivoja varnosti informacij morajo biti vključeni vsi zaposleni in pogodbeni sodelavci. Naloga izvajalcev zdravstvene dejavnosti je, da CIZ sporočajo opažene varnostne incidente, kot so:

- varnostne pomanjkljivosti
- namerne ali nenamerne varnostne kršitve
- nepravilno ali sumljivo delovanje informacijskih sistemov
- nedelovanje informacijskih sistemov
- kršitve določil SUVI

O varnostnih incidentih in varnostnih pomanjkljivostih se vodi zapise ter se jih predstavi na vodstvenem pregledu in poroča CIZ.

1.7 UPRAVLJANJE Z DOKUMENTI POLITIKE VAROVANJA INFORMACIJ

Dokumenti politike varovanja informacij so objavljeni v elektronski obliki na način, da so dostopni vsem izvajalcem zdravstvene dejavnosti, ki se vključujejo v eZdravje. Skrbništvo vsakega posameznega dokumenta politike varovanja informacij je na strani pooblaščenih oseb CIZ, ki so zadolžene za njegovo pravočasno obnavljanje, spreminjanje ter objavo.

1.8 VZDRŽEVANJE POLITIKE VAROVANJA INFORMACIJ

Ob spremembah zakonodaje, pojavu novih groženj, novih varnostnih incidentov, spremembah organizacijske ali tehnične infrastrukture, ki vplivajo na varovanje informacij in informacijskih sistemov, se bo SUVI nenehno prilagajal z uvajanjem novih in dopolnjevanjem že obstoječih varnostnih ukrepov in postopkov. Dinamično prilagajanje politik varovanja informacij ter postopkov in navodil za varovanje informacij v skladu z novimi zahtevami in spremembami, ki vplivajo na oceno varnostnega tveganja, je zadolžitev pooblaščenih oseb CIZ. SUVI mora biti skladen z veljavno zakonodajo ter mora upoštevati priporočila standardov informacijske varnosti.

1.9 SANKCIJE

Vsako neupoštevanje določil politike varovanja informacij ter navodil in postopkov varovanja informacij se šteje za kršitev dela izvajalcev zdravstvene dejavnosti, ki so vključeni v eZdravje in se kot tako tudi sankcionira z ustreznimi ukrepi, ki jih določi Ministrstvo za zdravje.