

Naziv dokumenta: **KROVNA POLITIKA VAROVANJA INFORMACIJ IN UPRAVLJANJA
INFORMACIJSKE PODPORE**

Namen dokumenta: Dokument opisuje pravila varovanja informacij Onkološkega inštituta Ljubljana (OI)

Številka dokumenta: **2.0**

Številka zadeve: **5012-0001/2025**

Verzija: **3.2**

Število strani: 45

Referenčni dokument: Zakov o varstvu osebnih podatkov (ZVOP-2)
Zakon o zdravstveni dejavnosti (ZZDej)
Pravilnik o varstvu osebnih in drugih podatkov na Onkološkem inštitutu
Ljubljana z dne 03.07.2019

Dokument je namenjen zaposlenim na OI ter določenih pogodbenih obdelovalcev in sodelavcem OI
v zvezi z ukrepi in politikami za zagotavljanje informacijske varnosti OI.

Pregledal (skrbnik):

Skrbnik SUVI: Luka Fortuna

Odobril:

Zlata Štiblar Kisić
direktorica

Dne: 19. 12. 2025

Onkološki inštitut Ljubljana, Zaloška cesta 2, 1000 Ljubljana

E-pošta: info@onko-i.si
www.onko-i.si

KAZALO

1. UVOD	7
1.1. Vpetost v organizacijo	7
1.2. Optimalna vrednost.....	7
1.3. Celovito in skladno upravljanje tveganj	8
1.4. Vključenost deležnikov	8
1.5. Dostopnost in vključenost	9
1.6. Energetska učinkovitost	9
1.7. Upravljanje virov	9
1.8. Zmanjševanje papirne porabe.....	10
1.9. Družbena odgovornost.....	10
1.10. Organiziranost delovanja.....	10
2. POLITIKA KLASIFIKACIJE INFORMACIJ	12
2.1. Terminološki slovar	12
2.2. Namen politike klasifikacije informacij.....	12
2.3. Skrbništvo informacij.....	12
2.3.1. Osebni podatki	12
2.3.2. Občutljivi osebni podatki.....	12
2.3.3. Področja zbirk osebnih podatkov	12
2.3.4. Poslovna skrivnost.....	13
2.4. Javno.....	13
2.5. Skrbništvo in uporabniške pravice	13
2.6. Odgovornosti uporabnikov informacij	13
2.7. Označevanje informacij	13
2.8. Nadzor	13
3. POLITIKA FIZIČNE ZAŠČITE IN FIZIČNEGA DOSTOPA	14
3.1. Terminološki slovar	14
3.2. Namen politike fizične zaščite in fizičnega dostopa	14
3.3. Fizični dostop do varovanih območij.....	14
3.4. Politika čiste mize	14
3.5. Politika praznega zaslona	14
3.6. Odstranjevanje dokumentacije	15
3.7. Politika proti zlorabi opreme računalniškega informacijskega sistema	15
3.8. Nadzor nad fizičnim dostopom	15
4. POLITIKA DOSTOPA DO INFORMACIJ, APLIKACIJ IN INFORMACIJSKIH SISTEMOV	16
4.1. Terminološki slovar	16

4.2. Namen politike dostopa do informacij, aplikacij in informacijskih sistemov	16
4.3. Dostop do informacij, aplikacij in sistemov	16
4.4. Dodelitev pravic dostopa	17
4.5. Spremembe pravic dostopa	17
4.6. Ukinitev pravic dostopa	17
4.7. Nadzor nad pravicami dostopa do informacij, aplikacij in sistemov	18
5. POLITIKA DOSTOPA DO OMREŽJA	19
5.1. Terminološki slovar	19
5.2. Namen politike nadzora dostopa do omrežja	19
5.3. Varnost omrežja OI in dostop do omrežja	19
5.4. Oddaljen dostop do omrežja OI	19
5.5. Nadzor dostopov do omrežja OI	20
6. POLITIKA RAZVOJA, SPREMINJANJA IN VZDRŽEVANJA APLIKACIJ	21
6.1. Terminološki slovar	21
6.2. Namen politike za razvoj, spreminjanje in vzdrževanje aplikacij	21
6.3. Izvajanje razvoja aplikacij	21
6.4. Izbira pogodbenega sodelavca za razvoj aplikacije	21
6.4.1. Razvoj aplikacije	21
6.4.2. Dokumentacija aplikacije	22
6.4.3. Testiranje aplikacije	22
6.4.4. Prezem aplikacije	22
6.4.5. Uvajanje uporabnikov za delo na aplikaciji	22
6.5. Spreminjanje aplikacije	22
6.6. Vzdrževanje aplikacij	22
6.7. Nadzor	23
7. POLITIKA SPREMEMB INFORMACIJSKEGA SISTEMA	24
7.1. Terminološki slovar	24
7.2. Namen politike za nadzor sprememb informacijskega sistema	24
7.3. Nabava programske in strojne opreme	24
7.4. Namestitev programske in strojne opreme	24
7.5. Nadzor nad verzijami programske opreme	24
7.6. Nadzor sprememb informacijskega sistema	24
7.7. Upoštevanje trenutnih in bodočih potreb	24
8. POLITIKA DNEVNIKOV OBDELAV / REVIZIJSKIH SLEDI	26
8.1. Terminološki slovar	26
8.2. Namen politike za zagotavljanje revizijskih sledi	26

8.3. Skladnost in nadzor	26
8.4. Zagotavljanje revizijskih sledi	26
8.5. Sledljivost obdelav osebnih podatkov, občutljivih osebnih podatkov in poslovne skrivnosti ...	27
8.5.1. Osebni podatki in poslovna skrivnost.....	27
8.5.2. Občutljivi varovani osebni podatki	27
8.6. Sledljivost aktivnosti uporabnikov informacijskih storitev z administrativnimi računi.....	27
8.7. Dostop do hrambe podatkov o dostopih (vpogledih)	27
8.8. Nadzor	28
9. POLITIKA UPORABE STORITEV INTERNETA.....	29
9.1. Terminološki slovar	29
9.2. Namen politike za uporabo storitev interneta	29
9.3. Uporaba storitev interneta.....	29
9.4. Uporaba svetovnega spleta (www)	29
9.5. Omejevanje dostopa do svetovnega spleta	29
9.6. Politika uporabe elektronske pošte.....	29
9.7. Omejevanje uporabe elektronske pošte	30
9.8. Nadzor uporabe storitev interneta	30
10. POLITIKA UPRAVLJANJA IN VAROVANJA GESEL	31
10.1. Terminološki slovar	31
10.2. Namen politike upravljanja in varovanja gesel	31
10.3. Varno ravnanje z gesli	31
10.4. Redna menjava in izbira kakovostnega gesla	31
10.5. Dodatna pravila za izbiro gesel in hramba gesel za administratorske račune	32
10.6. Izbira in menjava gesel kontrole fizičnega dostopa (alarmni sistem)	32
10.7. Neupravičeno ravnanje z geslom oziroma uporabniškim imenom.....	32
10.8. Nadzor nad upravljanjem z gesli	32
11. POLITIKA VAROVANJA V POVEZAVI Z ZAPOSLENIMI	33
11.1. Terminološki slovar	33
11.2. Namen politike varovanja v zvezi z zaposlenimi	33
11.3. Izobraževanje, usposabljanje in preverjanje	33
11.4. Varovanje informacij na OI	33
11.5. Postopki pred zaposlitvijo	33
11.6. Postopki med zaposlitvijo.....	33
11.7. Postopki ob prekinitvi zaposlitve.....	33
11.8. Odgovornost zaposlenih OI	33
12. POLITIKA UPRAVLJANJA KAKOVOSTI IN VARNOSTI STORITEV POGODBENIH SODELAVCEV	34

12.1. Terminološki slovar	34
12.2. Namen politike za upravljanje kakovosti in varnosti pogodbenih sodelavcev.....	34
12.3. Pogodbeno urejanje razmerij s pogodbenimi sodelavci	34
12.4. Upravljanje sprememb storitev pogodbenih sodelavcev.....	35
12.5. Nadzor pogodbenih sodelavcev	35
12.6. Nabava naprav ali storitev ter sodelovanje z dobavitelji oz. zunanjimi izvajalci.....	35
13. POLITIKA ZAŠČITE DELOVANJA INFORMACIJSKEGA SISTEMA	36
13.1. Terminološki slovar	36
13.2. Namen politike za zaščito informacijskih sistemov.....	36
13.3. Infrastruktura	36
13.4. Zagotavljanje kakovosti infrastrukture.....	36
14. POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO	37
14.1. Terminološki slovar	37
14.2. Namen politike zaščite pred zlonamerno programsko kodo	37
14.3. Zaščita pred zlonamerno programsko opremo	37
15. POLITIKA IZDELAVE IN SHRANJEVANJA VARNOSTNIH KOPIJ	38
15.1. Terminološki slovar	38
15.2. Namen delovnega navodila za izdelavo in shranjevanje varnostnih kopij.....	38
15.3. Izdelava varnostnih kopij podatkov na strežnikih	38
15.4. Shranjevanje varnostnih kopij	38
15.5. Preverjanje varnostnih kopij	38
15.6. Nadzor izvajanja in shranjevanja varnostnih kopij.....	38
16. POLITIKA IZDELAVE IN SHRANJEVANJA ARHIVSKIH DOKUMENTOV.....	39
16.1. Terminološki slovar	39
16.2. Namen politike za izdelavo in shranjevanje dokumentov.....	39
16.3. Izdelava in hramba dokumentov.....	39
16.4. Izdelava in hramba dokumentov v papirni obliki	39
16.5. Izdelava in hramba dokumentov v elektronski obliki.....	39
17. POLITIKA UPRAVLJANJA Z VARNOSTNIMI INCIDENTI	40
17.1. Terminološki slovar	40
17.2. Namen politike za upravljanje varnostnih incidentov.....	40
17.3. Definicija incidenta.....	40
17.4. Prijava in beleženje incidentov.....	40
17.5. Ukrepanje v primeru pojava incidenta	40
17.5.1. Ukrepanje v primeru izgube, uničenja ali zlorabe osebnih podatkov, občutljivih osebnih podatkov in zaupnih podatkov	41

17.5.2. Ukrepanje v primeru poškodovanja, zlorabe ali izpada delovanja informacijskega sistema ter kraje programske in strojne opreme	42
17.5.3. Ukrepanje v primeru kršenja zakonodaje	42
17.5.4. Ukrepanje v primeru neupoštevanja postopkov varovanja informacij.....	42
17.6. Pregledovanje in ocena incidentov	42
18. POLITIKA UPORABE ZASEBNIH NAPRAV (BYOD) V DELOVNEM OKOLJU	43
18.1. Terminološki slovar	43
18.2. Namen politike uporabe zasebnih naprav (BYOD) v delovnem okolju	43
18.3. Zahteve za uporabo zasebnih naprav v delovnem okolju	43
18.4. Register odobrenih VPN dostopov in njihovih uporabnikov	43
18.5. Prijava in beleženje incidentov.....	43
19. SKLADNOST IN MERLJIVOST	44
19.1. Namen politike skladnosti in merljivosti	44
19.2. Merljivost.....	44
19.3. Skladnost	44
19.4. Zagotavljanje kakovosti	44
19.5. Upravljanje podatkovnih virov	45

UVOD

Namen:

Temeljni namen in načela delovanja informacijske podpore OI

1.1. VPETOST V ORGANIZACIJO

Onkološki inštitut Ljubljana (v nadaljevanju tudi OI ali organizacija), zagotavlja dosleden pristop k razvoju in izvajanju informacijske podpore ter varovanju informacij. Sistem je v celoti integriran s strategijo in potrebami OI ter usklajen s pristopom upravljanja OI, kar se zagotavlja z rednim poročanjem poslovnim in strokovnim organom OI. Vse pomembne odločitve v zvezi z informacijsko podporo se sprejemajo v skladu s strategijami in cilji OI.

Vsi procesi povezani z informacijsko podporo, se učinkovito in pregledno nadzorujejo s strani strokovnega direktorja in direktorja, strokovnega sveta in sveta zavoda. Informacijska podpora, je potrjeno skladna z veljavnimi predpisi EU in RS ter mednarodnimi in evropskimi standardi, smernicami in priporočili.

1.2. OPTIMALNA VREDNOST

OI zagotavlja optimalno vrednost storitev in sredstev informacijske podpore, ter njihovo stroškovno učinkovitost. Akcijski načrti in projektna dokumentacija vsebujejo zanesljivo in natančno sliko stroškov in pričakovanih koristi tako, da so medicinske in poslovne potrebe podprte učinkovito in uspešno, ter stroški informacijske podpore v največji možni meri optimizirani.

OI si prizadeva za stalno izboljševanje uspešnosti bolnišničnega, kemoterapijskega, lekarniškega sistema, sistema RIS/NIS/PACS in drugih zdravstvenih in poslovnih sistemov v skladu s strategijo delovanja informacijske podpore OI. Ključna so predvsem sledeča načela:

- analiza individualne uspešnosti programov, produktov in storitev: Redno se spremlja in ocenjuje uspešnost vsakega posameznega programa, produkta in storitve v OI. Na ta način se zagotavlja transparentnost in razumevanje doprinosa vsakega elementa k celotnemu portfelju programov, produktov in storitev;
- prilagajanje celotnega portfelja programov, produktov in storitev glede na spreminjajoče se prioritete in povpraševanje: Prioritete in potrebe OI se nenehno spreminjajo. Zato se portfelj programov, produktov in storitev prilagaja v skladu s spremembami v strategiji OI, sprejetimi finančnimi načrti ter aktualnimi zahtevami trga, ter se na ta način neprestano zagotavlja največjo vrednost za vse deležnike;
- optimizacija uspešnosti celotnega portfelja: Na podlagi analize posameznih elementov portfelja se izvajajo ukrepi za optimizacijo celotne uspešnosti portfelja programov, produktov in storitev. To lahko vključuje preusmerjanje virov, prilagoditev prioritet, optimizacijo procesov ali kakršne koli druge ukrepe, ki prispevajo k izboljšanju učinkovitosti in uspešnosti;
- spremljanje in izboljševanje: Stalno se spremlja učinkovitost ukrepov za optimizacijo portfelja programov, produktov in storitev ter izvaja potrebne prilagoditve in izboljšave, da se zagotovi dosledno izpolnjevanje ciljev OI;
- z zavezo k stalnemu izboljševanju in prilagajanju portfelja programov, produktov in storitev se zagotavlja, da OI uspešno sledi spremenljivim zahtevam in dosega svoje cilje.

OI si prizadeva za učinkovito uresničevanje ciljev ob minimaliziranju tveganj in maksimiziranju dolgoročnih koristi. Ključna so predvsem sledeča načela:

- izboljšana komunikacija z deležniki: Vloga sev učinkovito komunikacijo z vsemi vpletenimi deležniki, vključno s končnimi uporabniki. Deležnike se redno informira o napredku, potrebah in pričakovanjih ter se s tem zagotavlja jasno razumevanje in podporo skozi celoten proces;

- povečana vključenost deležnikov: Aktivno se vključuje vse relevantne deležnike v proces načrtovanja, razvoja in implementacije programov, produktov in storitev. S tem se zagotavlja, da so potrebe in pričakovanja deležnikov ustrezno upoštevane, kar vodi k boljši sprejetosti in uspehu programov, produktov in storitev;
- zagotavljanje vrednosti in kakovosti rešitev in storitev: Stremi se k zagotavljanju visoke vrednosti in kakovosti vseh programov in storitev. To se doseže z jasno opredeljenimi cilji, rednim spremljanjem izvajanja in zagotavljanjem skladnosti z najboljšimi praksami in standardi;
- maksimiranje prispevka : Vrednoti se projektni prispevek posameznih programov, produktov in storitev. S prilagajanjem projektov glede na prioritetne naloge in strateške cilje organizacije, se maksimira njihov skupni prispevek k uspehu organizacije.

1.3. CELOVITO IN SKLADNO UPRAVLJANJE TVEGANJ

Upravljanje tveganj informacijske podpore, je ključni element zagotavljanja varnosti in zanesljivosti informacijskih sistemov v OI. Zagotovljeno je upravljanje tveganj glede informacijske podpore skladno s pravili obvladovanja tveganj OI. Proces vključuje identifikacijo, analizo in oceno tveganj, ki bi lahko vplivala na informacijsko podporo, ter razvoj strategij za njihovo obvladovanje ali zmanjšanje. Cilj je zagotoviti, da so informacijski sistemi odporni proti grožnjam, kot so kibernetični napadi, napake v programski opremi, človeške napake in naravne katastrofe.

Upravljanje tveganj se začne z določitvijo obsega in ciljev procesa, ki mu sledi zbiranje podatkov o obstoječem informacijskem okolju in potencialnih grožnjah. Nato se izvede ocena tveganj, kjer se identificirana tveganja ocenijo glede na njihovo verjetnost in potencialni vpliv na organizacijo. Na podlagi te ocene se razvijejo strategije za obvladovanje tveganj, ki lahko vključujejo tehnične, organizacijske in proceduralne ukrepe. Tveganja na področju informacijske podpore so ažurno vodena, kot del Centralnega registra tveganj OI.

Proces upravljanja tveganj je dinamičen in se redno posodablja, da odraža spremembe v informacijskem okolju in pojav novih groženj. OI uporablja sistematičen pristop k upravljanju tveganj, ki vključuje stalno spremljanje in pregledovanje varnostnih ukrepov, ter prilagajanje internih aktov, politik in postopkov, ko je to potrebno.

1.4. VKLJUČENOST DELEŽNIKOV

Vsi zainteresirani deležniki podpirajo strategijo in akcijske načrte informacijske podpore. Komunikacija z deležniki (predstavitve različnim deležnikom, obravnava na strokovnem svetu in svetu zavoda, ter druge sorodne aktivnosti) je učinkovita in pravočasna, ter je osnova za poročanje vzpostavljena za povečanje uspešnosti.

OI si prizadeva za učinkovito vključitev kadra / človeških virov (notranjih in zunanjih) v skladu z namenom doseganja ciljev OI in te politike. Ključna so predvsem sledeča načela:

- načrtovanje in razvoj posameznikov oz. deležnikov: OI skrbi za sistematično načrtovanje in razvoj posameznikov oz. deležnikov. To vključuje identifikacijo ključnih kompetenc in veščin, potrebnih za doseganje ciljev OI, ter zagotavljanje ustrezne usposobljenosti in razvoja posameznikov oz. deležnikov;
- z namenom zmanjšanja možnosti nepooblaščenega spreminjanja in/ali zlorabe informacij ali storitev in zanašanja na ključne posameznike, OI zagotavlja, kolikor je mogoče in izvedljivo ločeno upravljanje in/ali izvajanje nekaterih nalog ali področij odgovornosti (razdelitev skrbništva na več skrbnikov) ter hkrati skrbi tudi za področje upravljanja razvoja ključnega kadra (kot npr. deljenje znanja, nasledstvo, zadostno število usposobljenega kadra ipd.);

- učinkovita porazdelitev virov: V OI se spremljajo potrebe in zahteve posameznih projektov, področij dela in funkcij, ter se zagotavlja ustrezno porazdelitev posameznikov oz. deležnikov v skladu s strategijo in cilji OI. Pri tem se upošteva tako obstoječe, kot tudi potencialne potrebe in priložnosti za rast;
- spodbujanje sodelovanja in timskega dela: OI verjame v pomen sodelovanja in timskih prizadevanj pri doseganju ciljev organizacije. Zato se spodbuja kultura sodelovanja, deljenja znanja in izkušenj, ter ustvarjanja motivacijskega okolja, ki omogoča razvoj in rast posameznikov in ekip;
- neprekinjeno izboljševanje: V OI se spremlja uspešnost pristopov k upravljanju kadra, ter se neprestano išče priložnosti za izboljšanje. To vključuje prepoznavanje in odpravljanje morebitnih ovir ter izvajanje ukrepov za povečanje učinkovitosti in zadovoljstva posameznikov oz. deležnikov;
- z zavezo k učinkovitemu upravljanju kadra, se zagotavlja opremljenost posameznikov oz. deležnikov s potrebnim znanjem, kompetencami, motivacijo in podporo, ter izpolnjevanje tudi vseh zahtevanih pogojev te politike in OI, da lahko uspešno prispevajo k doseganju ciljev OI.

1.5. DOSTOPNOST IN VKLJUČENOST

Informacijska podpora OI skrbi, da se zagotavlja enakopravna dostopnost, preprečuje pristranskost pri strokovni in poslovni uporabi informacijske podpore in tako preprečuje diskriminacijo ali kakršnokoli neupravičeno razlikovanje pacientov, zaposlenih, zunanjih sodelavcev, dobaviteljev in tretjih oseb. Informacijska podpora zagotavlja enakopraven dostop do znanja, podatkov in storitev OI, ter odpravlja ovire za kakovostno in varno uporabo. OI in z njim celovita informacijska podpora sta zavezana k skrbnemu delovnemu okolju, kjer so individualne razlike cenjene na vseh ravneh organizacije. Potrebe po kakovostnem, varnem in enakopravnem delovanju se obravnava na vseh možnih korakih za paciente in osebe.

1.6. ENERGETSKA UČINKOVITOST

Ena izmed ključnih komponent trajnostne informacijske podpore je povečanje energetske učinkovitosti. To vključuje optimizacijo podatkovnih centrov, računalniških sistemov in omrežne infrastrukture za zmanjšanje porabe energije. Napredne tehnologije hladilnih sistemov, virtualizacija strežnikov in uporaba obnovljivih virov energije so dobre prakse, ki na OI pomembno prispevajo k zmanjšanju ogljičnega odtisa informacijske podpore.

1.7. UPRAVLJANJE VIROV

V OI se pravočasno identificirajo potrebe, zagotavljanje infrastrukture in človeških virov, ki so potrebni za načrtovanje, izvedbo, vzdrževanje in stalno izboljševanje sistema, za upravljanje varovanja informacij.

Ključna so predvsem sledeča načela:

- zagotavljanje optimalnih potreb po virih: Cilj je zagotoviti, da so potrebe po virih organizacije ustrezno zadovoljene. To pomeni, da se s pravilnim načrtovanjem in upravljanjem s sredstvi, vključno z denarnimi sredstvi, človeškimi viri in infrastrukturo, omogoči nemoten potek poslovanja;
- optimizacija stroškov I&T: Zavezo k stalnemu izboljševanju učinkovitosti in optimizaciji stroškov na področju informacijske tehnologije, se dosega z racionalizacijo procesov, uporabo ustrezne tehnologije ter doslednim nadzorom nad stroški, ne da bi pri tem ogrozili kakovost ali varnost informacijskih sistemov;
- povečanje verjetnosti uresničitve koristi: Pri načrtovanju in izvajanju projektov na področju informacijske tehnologije se pozornost namenja zagotavljanju konkretnih koristi za OI. Z

vzpostavitev jasnih meril za uspeh projektov ter rednim spremljanjem napredka se povečuje verjetnost uresničitve koristi in doseganja pričakovanih rezultatov;

- pripravljenost za prihodnje spremembe: OI se zaveda hitrih sprememb v tehnološkem okolju in poslovnih potrebah. Zato se stalno sledi trendom in inovacijam na področju informacijske tehnologije ter prilagaja procese in storitve, da so pripravljeni na prihodnje spremembe in izzive.

OI je kot pomembne, prepoznal tudi trajnostne vidike informacijske podpore, ki zajemajo odgovorno upravljanje z IT sredstvi oz. drugimi viri skozi celoten življenjski cikel, od nabave do odstranitve/uničenja. To vključuje izbiro izdelkov z daljšo življenjsko dobo, podporo za ponovno uporabo in recikliranje starih naprav ter izogibanje elektronskim odpadkom.

1.8. ZMANJŠEVANJE PAPIRNE PORABE

Digitalizacija procesov in prehod na brezpapirno poslovanje sta pomembna elementa trajnostne informacijske podpore OI, ki pomagata zmanjševati porabo papirja in vpliv na gozdove. To ne samo, da zmanjšuje okoljski odtis OI, temveč tudi povečuje učinkovitost in dostopnost informacij.

1.9. DRUŽBENA ODGOVORNOST

Vključevanje trajnostnih praks v strategijo informacijske podpore ni le koristno za okolje, ampak lahko prinese tudi ekonomske prednosti, kot so zmanjšani operativni stroški in izboljšana podoba OI. OI se zavedajo svoje vloge v okoljskih vprašanjih in prevzemajo odgovornost za vključevanje trajnostnih vidikov v informacijsko podporo.

1.10. ORGANIZIRANOST DELOVANJA

V OI je oblikovan sistem upravljanja področja varovanja informacij in informacijske podpore na podlagi ciljev organizacije in skladno s smernicami informacijske varnosti, ter predmetno politiko.

Ključna so predvsem sledeča načela:

- spodbujanje komuniciranja o ciljih predmetne politike vsem deležnikom, kot tudi o pomembnih odločitvah povezanih s področjem varovanja informacij in informacijsko podporo ter njihovem vplivu na OI;
- opredelitev ciljne ravni zmogljivosti procesov in prioritete izvedbe; uvedba posebne organizacijske strukture za upravljanje področja varovanja informacij in informacijske podpore, ki omogoča učinkovito in strokovno sprejemanje odločitev;
- vključenost potrebne tehnologije in znanja o informacijski tehnologiji in varovanju informacij v organizacijsko strukturo; opredelitev, dodelitev vlog in odgovornosti na področju varovanja informacij in informacijske podpore, vključno z nivoji pooblastil in odgovornostjo;
- opredelitev in vzdrževanje odgovornosti lastništva informacij (podatkov) ter informacijskih sistemov; klasifikacija informacij in informacijskih sistemov, ter njihova zaščita skladno s klasifikacijo;
- opredelitev potrebnih veščin in kompetenc za doseg ciljev skladno s predmetnimi politikami; uvedba postopkov za vzdrževanje skladnosti z veljavno zakonodajo, sprejetimi politikami, standardi in smernicami s področja varovanja informacij ter informacijske podpore; uvedba posledic in odgovornosti za neupoštevanje zakonodaje;
- spremljanje trendov in novosti na področju varovanja informacij in informacijske podpore, ter njihovo upoštevanje pri prihodnjem oblikovanju in izboljšanju okvira nadzora;

- načrtovanje, zasnova in izvedba procesov ter infrastrukture za podporo (npr. sistem za upravljanje tveganj, informacijska orodja za vodenje projektov, informacijska orodja za nadzor stroškov, informacijska orodja za spremljanje incidentov ipd.);
- neprestana izboljšava procesov na področju varovanja informacij in informacijske podpore.

POLITIKA KLASIFIKACIJE INFORMACIJ

Namen:

Opis pravil klasificiranja podatkov Onkološkega inštituta Ljubljana

2.1. TERMINOLOŠKI SLOVAR

Klasifikacija informacij razvrstitev podatkov glede na varnostne zahteve.

2.2. NAMEN POLITIKE KLASIFIKACIJE INFORMACIJ

Politika klasifikacije informacij določa pravila in postopke klasifikacije podatkov ter odgovornosti pri njihovem upravljanju. Pravila in postopki zmanjšajo možnost nepooblaščne uporabe, ki ima lahko za posledico razkritje osebnih podatkov, občutljivih osebnih podatkov in poslovne skrivnosti.

2.3. SKRBNIŠTVO INFORMACIJ

OI upravlja z informacijami, ki se nahajajo na medijih OI, s katerimi se izvajajo poslovni procesi. To so informacije, ki se uporabljajo za izvrševanje delovnih nalog. Na OI se nahajajo sklopi informacij, ki jih klasificiramo kot:

2.3.1. Osebni podatki

Osebni podatki se uporabljajo v poslovnih procesih OI in se nanašajo na posameznika (zaposlenega, pogodbenega sodelavca, uporabnika storitev). Osebnostne podatke lahko obdelujejo le uporabniki informacijskih storitev OI Ljubljana, zaradi izvajanja delovnih obveznosti. Osebnostne podatke se varuje v območjih prostorov zdravstvene dejavnosti, upravne dejavnosti in računalniškega informacijskega sistema ter komunikacijskega sistema. Zloraba osebnih podatkov oziroma nepooblaščen vdor ali dostop v zbirko osebnih podatkov ter njihovo razkritje se šteje za hujšo kršitev delovnih obveznosti.

2.3.2. Občutljivi osebni podatki

Občutljivi osebni podatki v okviru OI se nanašajo predvsem na zdravstvene podatke, ki razkrivajo zdravstveno stanje posameznika, vključno z informacijami o diagnozah, terapijah, medicinskih postopkih in izvidih. Ti podatki so bistveni za zagotavljanje kakovostne zdravstvene oskrbe in obravnave pacientov ter se obdelujejo izključno v skladu z veljavno zakonodajo, kot so Zakon o varstvu osebnih podatkov, Zakon o pacientovih pravicah, Zakon o zdravstveni dejavnosti, itd.

Zdravstveni podatki iz baz podatkov, ki se vodijo v okviru OI, vključujejo podatke o preteklih zdravstvenih obravnavah, napotitvah, anamnezi, alergijah, operacijah, laboratorijskih izvidih in zdravilih, ki jih pacienti prejemajo. Ti podatki so ključni za koordinacijo oskrbe in nadaljnje zdravljenje ter se obdelujejo in shranjujejo v varovanih informacijskih sistemih, skladno z načeli zaupnosti in varnosti.

Občutljivi osebni podatki se hranijo in varujejo v varovanih prostorih (predalniki, omare, varne baze podatkov) in informacijskih sistemih. Dostop do teh podatkov je omogočen le pooblaščenim osebam in sicer tistim, ki so pooblaščen za obdelavo podatkov v skladu z internimi pravili bolnišnice in zakonodajo, kot to določa Zakon o varstvu podatkov in drugi relevantni predpisi. To vključuje, poleg zdravstvenih delavcev, tudi druge pooblaščen osebe (npr. osebje, ki je zadolženo za informacijske sisteme, administrativno podporo ali pravne službe), ki morajo do teh podatkov dostopati za namene zagotavljanja nemotenega izvajanja zdravstvene oskrbe in z njo povezanih storitev. Vsakršna zloraba, nepooblaščen dostop ali razkritje občutljivih osebnih podatkov, se šteje za hudo kršitev delovnih obveznosti in se obravnava skladno z zakonodajo.

2.3.3. Področja zbirk osebnih podatkov

OI vodi zbirke osebnih podatkov na področjih poslovne, strokovne medicinske in raziskovalne dejavnosti. Te zbirke so podrobno opisane v Katalogu evidenc obdelave osebnih podatkov, ki ga vodi inštitut skladno z zakonodajo.

Pravna podlaga za vodenje teh zbirk in obdelavo osebnih podatkov izhaja iz veljavnih predpisov, kot so Zakon o pacientovih pravicah, Zakon o zdravstveni dejavnosti, Zakon o varstvu osebnih podatkov ter drugi predpisi s področja zdravstvenega varstva, delovnega in davčnega prava, informacijske varnosti in znanstveno-raziskovalne dejavnosti. Podatki se obdelujejo tudi za namene izvajanja raziskovalnih in kliničnih študij, ob upoštevanju veljavnih pravnih podlag, ter etičnih in zakonskih smernic.

Dostop do osebnih podatkov je dovoljen le pooblaščenim osebam v skladu z notranjimi pravili in zakonodajo, pri čemer se zagotavlja najvišja stopnja varstva in varnosti podatkov. Vse zbirke so ustrezno zavarovane z varnostnimi ukrepi, ki vključujejo fizične in tehnične zaščitne ukrepe, da se prepreči nepooblaščen dostop, razkritje ali zloraba.

Vse obdelave osebnih podatkov so usklajene z zakonodajo in internimi politikami bolnišnice ter se izvajajo izključno v okviru zakonitih in legitimnih namenov, kot so zdravstvena oskrba, raziskovalna dejavnost, upravljanje zdravstvenih storitev in druge z zakonom določene dejavnosti

2.3.4. Poslovna skrivnost

Zaposleni na OI so dolžni varovati podatke in informacije, ki so določeni kot poslovno skrivnost, in jih ne smejo razkrivati nepooblaščenim osebam. Za poslovno skrivnost se ne morejo določiti informacije, ki so po zakonu javne, ali informacije o kršitvi zakona. S poslovno skrivnostjo se ne smejo seznaniti tretje osebe, ki niso zaposlene na OI in tudi ne zaposleni na OI, ki teh informacij oz. listin ali predmetov ne potrebujejo pri svojem delu oz. v zvezi z opravljanjem svojih funkcij.

2.4. JAVNO

Vsi podatki, za katere pooblaščne osebe OI v okviru obstoječe zakonodaje in Pravilnika o varstvu osebnih in drugih podatkov na Onkološkem inštitutu Ljubljana določijo, da se jih sme javno objaviti. Primeri takšnih informacij so objave v medijih.

2.5. SKRBNİŠTVO IN UPORABNIŠKE PRAVICE

Do posameznih sklopov podatkov lahko dostopajo osebe, ki so za to pooblaščne na podlagi svojega delovnega mesta ali s strani vodstva OI. Pooblaščne osebe nato odločajo o tem, kdo pridobi dovoljenje dostopa do informacij in na kakšen način se bo s to informacijo ravnalo, glede na njeno klasifikacijo.

2.6. ODGOVORNOSTI UPORABNIKOV INFORMACIJ

Vsi zaposleni in pogodbeni sodelavci OI, ki pridejo v stik z osebnimi podatki, občutljivimi osebnimi podatki ter poslovno skrivnostjo, morajo ravnati v skladu v veljavno zakonodajo ter sprejetimi internimi pravili, ki opredeljujejo varovanje informacij ter učinkovito izvajati zahteve delovnih navodil, kot del vsakodnevnih nalog pri delu.

2.7. OZNAČEVANJE INFORMACIJ

Osebnosti podatki, občutljivi osebni podatki ter poslovna skrivnost, morajo biti od nastanka do uničenja obvladovani na način, da je zagotovljena sledljivost uporabe podatkov. Klasifikacijo dokumentov zagotovi Onkološki inštitut skladno z zakonodajo.

V primeru zahteve po javni objavi podatkov, se postopa v skladu s Pravilnikom o posredovanju informacij javnosti in zakonom, ki ureja dostop do javnih informacij.

2.8. NADZOR

Pooblaščenca oseba za sistem upravljanja z varovanjem informacij (SUVI) je v primeru ugotovljenih ali zaznanih incidentov dolžna preverjati upoštevanje klasifikacije informacij, ter v primeru zaznanega neustreznega ravnanja sprožiti postopke skladne s Politiko upravljanja varnostnih incidentov.

POLITIKA FIZIČNE ZAŠČITE IN FIZIČNEGA DOSTOPA

Namen: Opis pravil dostopanja do območij Onkološkega inštituta Ljubljana

3.1. TERMINOLOŠKI SLOVAR

Informacije in informacijski sistem: vsa dokumentacija in celoten računalniški informacijski sistem kjer se nahajajo vse informacije, s katerimi se izvajajo delovne obveznosti.

Kontrola dostopa: mehanizem, ki omogoči dostop do prostorov OI.

Strežniške in komunikacijske omare ter centralni podatkovni center na zunanji lokaciji: računalniška oprema, ki skrbi za delovanje informacijskega sistema in se nahaja v območju računalniškega informacijskega sistema in komunikacijskega sistema ter v upravnih pisarnah.

Komunikacijski kabli: omrežje, ki zagotavlja komunikacije med vsemi deli računalniške opreme v območju računalniškega informacijskega sistema in komunikacijskega sistema ter prostorih zdravstvene in upravne dejavnosti.

Samodejno zaklepanje: avtomatizirano zaklepanje računalniške opreme.

3.2. NAMEN POLITIKE FIZIČNE ZAŠČITE IN FIZIČNEGA DOSTOPA

Politika fizične zaščite in fizičnega dostopa določa pravila in postopke fizičnih dostopov do informacij, in informacijskega sistema OI. Nepooblaščen dostop do informacij in informacijskega sistema ima lahko za posledico razkritje podatkov OI, med katere spadajo osebni podatki in občutljivi osebni podatki ter poslovna skrivnost.

3.3. FIZIČNI DOSTOP DO VAROVANIH OBMOČIJ

Na OI se varuje dostope do prostorov z ukrepi, ki zagotavljajo primerno varovanje informacij in informacijskega sistema. Ukrepi varovanje posameznih prostorov se razlikujejo po tem, v kakšno območje ti prostori spadajo.

Podrobnosti so določene v dokumentu »Dostop do prostorov na OI Ljubljana«.

3.4. POLITIKA ČISTE MIZE

Zaposleni OI ne smejo brez nadzora puščati dokumentacije (papirni dokumenti, CD, DVD, USB ključi), na kateri so osebni podatki ali občutljivi osebni podatki ter poslovna skrivnost na pisarniških mizah ali drugih mestih, kamor lahko dostopajo nepooblaščen osebe (čistilni servis, kurirji, obiskovalci, itd). Dokumentacija mora biti vedno zaščitena pred vpogledom nepooblaščenih oseb.

Dokumentacijo morajo zaposleni OI varno shraniti po končanem delovnem času oziroma, ko dlje časa niso fizično prisotni v prostoru. Izven delovnega časa, mora biti vsa pisarniška oprema ali prostori, kjer se hrani dokumentacija z osebnimi podatki ali občutljivimi osebnimi podatki ter poslovno skrivnostjo zaklenjena, računalniška oprema pa poleg tega še programsko varovana (dostop omogočen izključno z uporabniškim imenom in geslom).

3.5. POLITIKA PRAZNEGA ZASLONA

Uporabniki informacijskih storitev OI morajo zagotoviti, da nepooblaščenim osebam ni omogočen vpogled na računalniške zaslone. Vpogled lahko v posameznih primerih dovolijo, 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 uporabniki informacijskih storitev OI zakleniti računalniško opremo (dostop omogočen izključno z uporabniškim imenom in geslom). V kolikor je odsotnost z delovnega mesta daljša od 10 minut se računalniška oprema samodejno zaklene.

3.6. ODSTRANJEVANJE DOKUMENTACIJE

Vsa dokumentacija z osebnimi podatki ali občutljivimi osebnimi podatki ter poslovno skrivnostjo se mora po preteku določene dobe arhiviranja uničiti ali presneti na način, ki onemogoči branje podatkov. Zaposleni OI dokumentacije z osebnimi podatki ali občutljivimi osebnimi podatki ter poslovno skrivnostjo, ne smejo odmetavati v koše za smeti ali predati nepooblaščenim osebam. Za odstranjevanje dokumentacije se mora uporabiti primerne mehanizme (namenska programska oprema za presnemavanje nosilcev podatkov, komisijski zapisnik o uničenju dokumentacije, uporaba pooblaščenih družb za uničenje papirne dokumentacije in elektronskih nosilcev podatkov), ki zagotavljajo, da ne more priti do zlorabe osebnih podatkov in občutljivih osebnih podatkov ter poslovne skrivnosti.

3.7. POLITIKA PROTI ZLORABI OPREME RAČUNALNIŠKEGA INFORMACIJSKEGA SISTEMA

Računalniška oprema se uporablja samo za službene namene. OI izvaja ukrepe za preprečevanje kraje opreme, kar se zagotavlja z nadzorom nad prostori (prisotnost uporabnikov informacijskih storitev med delovnim časom ter fizično in tehnično varovanje izven delovnega časa). Za premeščanje računalniške opreme so zadolženi zaposleni Sektorja za informatiko, ki vodijo evidenco o opremi računalniškega informacijskega sistema in beležijo spremembe v računalniškem informacijskem sistemu. Vzdržuje se popis sredstev opreme računalniškega informacijskega sistema, ki se preverja 1-krat letno.

3.8. NADZOR NAD FIZIČNIM DOSTOPOM

Ob odhodu ali spremembi delovnega mesta se dostopne pravice dodelijo ali odvzamejo v informacijskem sistemu za fizični dostop.

Skrbnik SUVI, je v primeru zaznanih incidentov skupaj z pogodbenimi sodelavci dolžan preverjati poskuse nepooblaščenih dostopov do območij OI. V primeru zaznanega nepooblaščenega dostopa sproži postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA DOSTOPA DO INFORMACIJ, APLIKACIJ IN INFORMACIJSKIH SISTEMOV

Namen: Opis pravil dostopanja do informacijskega sistema OI

4.1. TERMINOLOŠKI SLOVAR

Aplikacija: računalniški program, ki omogoča dostop do informacij OI.

Informacijski sistem: računalniški sistem, ki omogoča delovanje vseh aplikacij in storitev za zaposlene OI in pogodbenne sodelavce.

Uporabniško ime in geslo: mehanizem dostopa do informacijskega sistema, ki je značilen za vsakega posameznega zaposlenega in pogodbenega sodelavca.

Administratorski račun: račun skrbnika aplikacije ali sistema.

VPN dostop: varen dostop z oddaljene lokacije do informacijskega sistema.

Evidenca pravic: seznam vseh pravic (vlog) zaposlenih OI in pogodbenih sodelavcev.

Nepooblaščen dostop: vsak dostop do informacij, aplikacij in sistemov, ki ni skladen z evidenco pravic.

Zaznani 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.

Registracijska kartica (ImPrivata): kartica za registracijo prisotnosti in avtentikacijo uporabnika.

4.2. NAMEN POLITIKE DOSTOPA DO INFORMACIJ, APLIKACIJ IN INFORMACIJSKIH SISTEMOV

Politika dostopa do informacij, aplikacij in informacijskih sistemov, določa pravila in postopke dodeljevanja pravic in pooblastil za dostop ter odgovornosti pri njihovem izvajanju. Pravila in postopki omogočajo nadzor nad dostopi do informacij, aplikacij in informacijskega sistema ter zmanjšajo možnost nepooblaščenega dostopa, ki ima lahko za posledico razkritje, izgubo ali napake v podatkih.

Politika dostopa, določa tudi pravila in postopke varovanja informacij ter postopek notranje kontrole in pregled ustreznosti pravic dostopov do aplikacij.

Pri upravljanju z dostopi do informacij, aplikacij in informacijskih sistemov, se morajo upoštevati določila s področja zakonodaje o varstvu osebnih podatkov.

Politika velja za vse organizacijske enote na OI.

4.3. DOSTOP DO INFORMACIJ, APLIKACIJ IN SISTEMOV

Dostop do informacij, aplikacij in informacijskih sistemov, ki pomeni dostop do osebnih podatkov, občutljivih osebnih podatkov ter poslovne skrivnosti, je omogočen izključno z uporabniškim imenom in geslom oz. z registracijsko kartico, ki je določena oz. dodeljena za vsakega posameznega zaposlenega OI ali pogodbenega sodelavca.

Pravice za dostop se uporabniku informacijskih storitev določi glede na njegovo vlogo oziroma delovno mesto. Odobrene in dodeljene pravice omogočajo, da uporabnik dostopa do tistih informacij, aplikacij in informacijskih sistemov, ki jih potrebuje za izvajanje svojega dela.

Podrobnosti so določene v dokumentu »Uporabniški dostopi« ter dokumentu »Matrika dostopov«.

Gesla administratorskih računov, so shranjena za uporabo v nujnih primerih, kar opredeljuje Politika upravljanja in varovanja gesel. Administratorji (zaposleni OI ali pogodbeni sodelavci) uporabljajo vsak svoj uporabniški račun, ki ima administratorske pravice.

4.4. DODELITEV PRAVIC DOSTOPA

Ob sklenitvi delovnega razmerja ali sklenitvi nove avtorske ali podjemne pogodbe na OI, kadrovska služba ob pomoči nadrejenega novozaposlenega sproži postopek za dodelitev pravic dostopa. Pristopno kontrolo izvaja Tehničnovzdrževalna služba. Novi uporabnik storitev mora biti seznanjen z dokumentacijo varnostnih politik, ki jih mora upoštevati ter podpisati ustrezne sporazume o varovanju informacij (Izjava o varovanju osebnih podatkov in/ali Izjava o zaupnosti), v kolikor to ni že vključeno v pogodbi o zaposlitvi oz. podjemni pogodbi.

Pravice dostopa do informacij, aplikacij in informacijskih sistemov, ki jih novi uporabnik storitev potrebuje za izvajanje svojega dela so določene glede na delovno mesto ali pogodbene obveznosti. Dodatne pravice lahko določijo in odobrijo nadrejeni (najmanj vodje služb) novega zaposlenega ali skrbniki pogodbenega sodelavca. Odobreno zahtevo za dodelitev ali ukinjanje dostopa se posreduje v Sektor za informatiko, kjer so zadolženi za upravljanje pravic dostopa.

Zahteva za uporabniški dostop mora vsebovati naslednje podatke:

- komu se dostop omogoči – ime, priimek,
- kdaj naj se mu dostop omogoči,
- do katerih informacij, aplikacij in sistemov potrebuje dostop
- ali potrebuje VPN dostop,
- datum začetka in datum konca dostopa,
- številko zdravnika (šifro RIZDDZ) in številko profesionalne kartice, v primeru, da gre za dostop za zdravnika,
- številko profesionalne kartice, v primeru, da delavec le-to potrebuje pri svojem delu,
- mobilno telefonsko številko - opcijsko.

Zaposleni Sektorja za informatiko sporočijo uporabniška imena in gesla, ki jih novi zaposleni potrebuje, na način, da je prvotno geslo enkratno in ga zaposlencu posreduje nadrejeni ali pa opravi osebni prevzem gesla v Sektorju za informatiko. Pogodbenemu sodelavcu se uporabniško ime pošlje po elektronski pošti na uporabnikov elektronski naslov. Geslo se pogodbenemu sodelavcu pošlje preko sms sporočila na njegov mobilni telefon.

4.5. SPREMEMBE PRAVIC DOSTOPA

Uporabniku informacijskih storitev se v času njegove zaposlitve ali pogodbenega sodelovanja pravice do informacij, aplikacij in informacijskih sistemov lahko spremenijo. Zahteve za spremembe pravic dostopa do posameznega informacijskega sistema, vodja službe ali skrbnik pogodbenega sodelavca pisno posreduje v Sektor za informatiko, kjer so zadolženi za upravljanje pravic dostopa.

4.6. UKINITEV PRAVIC DOSTOPA

Pravice dostopa se uporabniku storitev ukinejo v primeru zlorabe pravic, prekinitvi delovnega razmerja ali prenehanju pogodbenega sodelovanja.

V primeru zlorabe pravic zaposleni Kadrovske službe, vodja oddelka ali skrbnik pogodbenega sodelavca pisno sporoči zaposlenim Sektorja za informatiko, ki urejajo pravice dostopa, da se takoj izvede ukinitve ali omejitve pravic dostopa. Zaposleni v Sektorju za informatiko so dolžni nemudoma izvesti ukrepe za preprečitev zlorab. Tovrstne dogodke je potrebno beležiti kot varnostne incidente.

Ob prekinitvi delovnega razmerja ali prenehanju pogodbenega sodelovanja pošlje Kadrovska služba OI zahtevek za ukinitve vseh pravic do dostopa, ki so bile uporabniku storitev dodeljene ob zaposlitvi oziroma pogodbenem sodelovanju in tekom njegovega dela. V zahtevku za ukinitve pravic se posreduje tudi datum prenehanja dela oziroma datum, ko se uporabniku storitev ukinejo ali omejijo pravice.

Zaposleni Sektorja za informatiko po prejemu zahtevku za ukinitve pravic dostopa ukinejo vse pravice dostopa do informacij, aplikacij in informacijskih sistemov skladno z zahtevkom.

4.7. NADZOR NAD PRAVICAMI DOSTOPA DO INFORMACIJ, APLIKACIJ IN SISTEMOV

Skrbnik SUVI je v primeru kršitve dostopa dolžan preverjati poskuse dostopov do informacij, aplikacij in informacijskih sistemov. V primeru zaznanega nepooblaščenega dostopa mora biti obveščena Komisija za varnostne incidente. Komisija opravi začetno oceno incidenta, nato pa se, če je to potrebno, v postopek vključi tudi pooblaščen oseb za varstvo osebnih podatkov (DPO), ki oceni vpliv incidenta na varstvo podatkov

Ob odhodu ali spremembi delovnega mesta se dostopne pravice dodelijo ali odvzamejo v sistemu aktivnega direktorija (AD) in ob tem preveri skladnost s standardi varnosti in varstva podatkov..

POLITIKA DOSTOPA DO OMREŽJA

Namen:

Opis pravil dostopanja do omrežja OI

5.1. TERMINOLOŠKI SLOVAR

Požarna pregrada: računalniška oprema, ki dovoljuje ali omejuje dostop do omrežja OI.

Mrežni priključki: priključki za žični dostop do omrežja OI.

Aktivna vrata: logična vrata, katera so dovoljena za dostop do posameznih aplikacij ali storitev.

Radijski vmesnik: dostop do brezžičnega omrežja.

Dostopna točka: mesto strojne opreme za brezžično omrežje.

VPN povezava: varna povezava z oddaljene lokacije do informacijskega sistema.

Administrativni dostop: dostop skrbnika aplikacije ali sistema.

5.2. NAMEN POLITIKE NADZORA DOSTOPA DO OMREŽJA

Namen nadzora dostopa do omrežja je preprečiti nepooblaščen dostop do omrežnih storitev z uporabo:

- ustreznih mehanizmov varovanja omrežja OI,
- ustreznih mehanizmov nadzorovanja dostopov uporabnikov informacijskih storitev.

5.3. VARNOST OMREŽJA OI IN DOSTOP DO OMREŽJA

Na OI se zagotavlja varnost omrežja in preprečuje nedovoljen promet v in iz omrežja, z uporabo mehanizma požarne pregrade.

Uporabniki storitev lahko dostopajo do omrežja v prostorih OI z neposredno priključitvijo v omrežje. Uporabljajo se varnostni mehanizmi za omejevanje dostopa:

- vsi mrežni priključki so dokumentirani, pri čemer je evidentirano, kateri priključki so aktivni oziroma porabljeni,
- izvaja se nadzor nad aktivnimi vrati priključnih stikal,
- mrežne opreme, ki ni v lasti OI, ni dovoljeno priklapljati v omrežje,
- mrežno opremo lahko priklapljajo samo zaposleni Sektorja za informatiko ali pogodbeni izvajalci Sektorja za informatiko.

V primeru brezžičnega omrežja OI se uporabljajo varnostni mehanizmi za omejevanje dostopa:

- radijski vmesnik je šifriran,
- zagotovljen mora biti nadzor nad dostopnimi točkami (dostopne točke se nahajajo v območju prostorov zdravstvene dejavnosti, upravne dejavnosti ali računalniškega informacijskega sistema in komunikacijskega sistema) (Politika fizične zaščite in fizičnega dostopa).

5.4. ODDALJEN DOSTOP DO OMREŽJA OI

Oddaljen dostop do omrežja za uporabnike storitev, se omogoči le tistim uporabnikom, ki ga potrebujejo pri svojem delu. Dodelitev oddaljenega dostopa poteka v skladu s Politiko nadzora dostopa informacij, aplikacij in sistemov.

Do omrežja uporabniki informacijskih storitev z oddaljenih lokacij dostopajo preko VPN povezave, ki se zaključi na požarni pregradi. Uporabniki storitev se morajo za vzpostavitev VPN povezave overiti najmanj z uporabniškim imenom in geslom. Do službene elektronske pošte, lahko zaposleni dostopajo preko HTTPS varne internetne povezave.

Uporabniki informacijskih storitev so dolžni pri oddaljenem dostopu zagotoviti ustrezno varnost informacij in informacijskih sistemov OI, oziroma preprečiti možnost nepooblaščenega dostopa do omrežja OI. Zato se morajo uporabljati varnostni mehanizmi:

- VPN povezave ni dovoljeno puščati vklopljene nenadzorovane,
- po končanem delu se je potrebno odjaviti iz omrežja in zagotoviti, da osebni podatki in občutljivi osebni podatki ter poslovna skrivnost ostanejo shranjeni izključno v omrežju, oziroma informacijskem sistemu OI in ne na računalniških napravah izven prostorov OI.

Pri oddaljenem dostopu je dovoljena uporaba aplikacij za oddaljeni dostop do namizja ali aplikacij za skupno rabo namizja pod pogojem, da je pri tem mogoče enolično določiti obe strani komunikacije. Dostopne podatke pogodbenim partnerjem posreduje zgolj Sektor za informatiko.

5.5. NADZOR DOSTOPOV DO OMREŽJA OI

Vsak dostop do omrežja se beleži. Dodatno se beležijo vsi administrativni dostopi do omrežja.

Skrbnik SUVI je v primeru zaznanih incidentov dolžna preveriti poskuse dostopov do omrežja. V primeru zaznanega nepooblaščenega dostopa mora sprožiti postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA RAZVOJA, SPREMINJANJA IN VZDRŽEVANJA APLIKACIJ

Namen:

Opis pravil obvladovanja razvoja in vzdrževanja aplikacij

6.1. TERMINOLOŠKI SLOVAR

Produksijsko okolje: okolje, kjer poteka obratovanje informacijskega sistema.

Testno okolje: okolje, kjer se opravljajo testi aplikacij pred sprejemom v obratovanje.

Razvojno okolje: okolje, kjer se izvaja razvoj aplikacij.

Glavni uporabnik: glavni uporabnik je uporabnik na OI s kompetencami za uporabo sistema.

6.2. NAMEN POLITIKE ZA RAZVOJ, SPREMINJANJE IN VZDRŽEVANJE APLIKACIJ

Namen politike je opredeliti postopek razvoja, spreminjanja in vzdrževanja aplikacij, odgovornosti in naloge uporabnikov informacijskih storitev, način nadzora ter dokumentacijo, ki jo je potrebno pri tem izdelati.

6.3. IZVAJANJE RAZVOJA APLIKACIJ

Razvoj aplikacij je projektno organiziran in se izvaja po predpisanih fazah in skladno z organizacijsko strukturo ter predpisanimi vlogami in odgovornostmi (odgovorne osebe, vodstvo, strokovni svet, svet zavoda). Razvoj se izvaja načrtno in postopno skladno z akcijskimi načrti, da se zagotovi uspešna digitalizacija OI, skladnost s strategijo OI in doseganje želene vrednosti postopnih sprememb.

Načrt in specifikacije morajo biti pripravljene na način, da dosegajo potrebne spremembe in inovacije izboljšano uporabniško izkušnjo ter izboljšano operativno učinkovitost in učinkovitost z izkoriščanjem razvoja IT in nastajajočih tehnologij. Zagotovljen mora biti agilen razvoj aplikacij in skrb za dostavo IT rešitev in storitev, ki omogočajo nadgradnje in razširitve.

Pri razvoju se upoštevajo vsa sredstva IT in optimizira vrednost, ki jo bo zagotavljala nova uporaba. Razvojna dokumentacija zagotavlja dovolj informacij o sredstvih storitve, da omogoči kasnejše učinkovito upravljanje storitve.

6.4. IZBIRA POGODBENEGA SODELAVCA ZA RAZVOJ APLIKACIJE

Okvir za naročanje storitev pri pogodbenih izvajalcih postavlja veljavna zakonodaja. V razpisni dokumentaciji se pri pogojih, ki jih mora izpolnjevati pogodbeni sodelavec, navede poleg zahtev o ustrezni funkcionalnosti in zmogljivosti aplikacije tudi zahteve glede izvajanja postopkov varovanja informacij OI in zagotavljanja storitve glede na toleriran čas izpada poslovnih procesov OI.

6.4.1. Razvoj aplikacije

Razvoj aplikacij poteka v razvojnem okolju pogodbenega sodelavca. Zaposleni Sektorja za informatiko in skrbnik pogodbenega sodelavca OI so odgovorni, da pogodbenega sodelavca že pred začetkom razvoja aplikacije seznani s postopki varovanja informacij, ki jih je dolžan upoštevati. Stalno se skrbi za ustrezno partnerstvo ter dvostranski pretok informacij, prenos znanja in veščin.

Stalno se spremlja učinkovita in uspešna uporaba virov, povezanih z IT, ter zagotavlja preglednost in odgovornost glede stroškov in uporabe javnih sredstev ter medicinske in poslovne vrednosti rešitev in storitev. V procesu razvoja aplikacije se stalno spremlja tveganje nepričakovanih zamud, stroškov in erozije vrednosti.

Pomemben del načrtovanja razvoja je skrb za informacijsko varnost, vključno s trenutnimi in pričakovanimi ravni pojavljanja incidentov, ter skrb za vgrajeno in privzeto zasebnost, kar so obvezni sestavni deli dokumentacije oziroma specifikacij.

Med razvojem aplikacije se skrbi za vključenost vseh potrebnih deležnikov, predvsem s poudarkom na komunikaciji s končnimi uporabniki in njihovo vključevanje v vse pomembne vsebinske odločitve.

6.4.2. Dokumentacija aplikacije

Dokumentacija nove aplikacije vsebuje vsaj:

- navodilo za namestitev aplikacije,
- enolična oznaka nove verzije aplikacije in opis sprememb nove verzije,
- opis tehničnih zahtev za strojno in programsko opremo strežnika, na katerem bo nameščena nova aplikacija,
- oceno izpolnjevanja zahtev informacijske varnosti,
- oceno izpolnjevanja zahtev varstva osebnih podatkov ter vgrajene in privzete zasebnosti,
- navodilo za testiranje vključno s testnimi scenariji,
- uporabniški priročnik za uporabnike, ki bodo uporabljali aplikacijo.

6.4.3. Testiranje aplikacije

Testiranje aplikacije je obvezna faza pred prenosom v produkcijsko okolje informacijskega sistema OI.

Prvo testiranje izvede pogodbeni sodelavec že v svojem okolju, z namenom odpraviti neskladnosti s specifikacijami aplikacije, ki so opredeljene v pogodbi.

Nadaljnje testiranje se izvede v testnem okolju informacijskega sistema OI, ki mora biti od produkcijskega okolja ločeno tako, da testiranje ne more vplivati na produkcijsko okolje informacijskega sistema. Testno okolje predstavlja simulacijo produkcijskega okolja. Testiranje izvede ključni uporabnik.

Ko se z ustreznim postopkom testiranja ugotovi, da izdelana aplikacija zagotavlja v pogodbi opredeljeno funkcionalnost, zmogljivost in varnostne zahteve, se podpiše končni prevzemni zapisnik in zaposleni Sektorja za informatiko v sodelovanju s pogodbenim sodelavcem OI prenesejo aplikacijo v produkcijsko okolje.

6.4.4. Prevzem aplikacije

Za prevzem aplikacije je odgovoren vodja Sektorja za informatiko, ki odobri namestitev aplikacije v produkcijsko okolje informacijskega sistema OI. Dobavitelj je dolžan pripraviti namestitveni paket.

6.4.5. Uvajanje uporabnikov za delo na aplikaciji

Pred ali po prenosu aplikacije v produkcijsko okolje se izvede usposabljanje uporabnikov za uporabo nove aplikacije ali sprememb nove verzije aplikacije. Pri šolanju sodeluje ključni uporabnik, ki je znanje prevzel od dobavitelja rešitve.

6.5. SPREMINJANJE APLIKACIJE

Spremembe aplikacije, lahko predlaga vsak uporabnik svojemu vodji enote/slужbe, pri čemer natančno obrazloži razlog za spremembo in predlaga želeni rok izvedbe. Vodja enote/slужbe predlog posreduje Sektorju za informatiko, ki ga preuči in poda realne možnosti izvedbe. Zaposleni Sektorja za informatiko so skupaj s ključnim uporabnikom odgovorni za pripravo specifikacij za spremembo aplikacij.

6.6. VZDRŽEVANJE APLIKACIJ

V kolikor uporabniki pri delu z aplikacijo naletijo na težave oziroma napake, jih sporočijo zaposlenim Sektorja za informatiko preko namenskega sistema za poročanje napak. Pri prijavi napake ali težave mora uporabnik navesti:

- ob kateri aktivnosti je prišlo do napake,
- kako se napaka odraža,
- če je možno tudi sliko zaslona v trenutku, ko se je napaka ali težava pojavila.

Če se ugotovi, da je napaka povezana z delovanjem aplikacije, se v reševanje vključi razvijalca aplikacije. Če je vzrok za težavo ali napako take narave, da zahteva spremembo aplikacije se sproži postopek za razvoj nove verzije aplikacije.

6.7. NADZOR

V primeru težav v delovanju, ki jih glede na obseg ali resnost nezmožnosti opravljanja poslovnih procesov lahko smatramo za izpad informacijskega sistema, mora biti o tem obveščen Skrbnik SUVI preko prijavnega obrazca za registracijo varnostnega incidenta.

V OI se zagotavlja celovit pogled na poslovno okolje in področja varovanja informacij in informacijske podpore, načrtovano smer ter ukrepe, ki so potrebni za uskladitev s smernicami, novimi standardi ter veljavno zakonodajo. Kot bistvena pri začrtani smeri se upošteva:

- raven digitalizacije, pri čemer se oceni t.i. trenutno digitalno zrelost organizacije, ter pripravi načrt za zapolnitev morebitne vrzeli do želene digitalne zrelosti organizacije. Prehod na višjo raven digitalizacije se upošteva v vseh delovnih procesih z namenom zagotoviti zanesljivo, hitro in učinkovito doseganje strateških ciljev;
- ocena učinkovitosti trenutnih storitev na področju informacijske tehnologije in razumevanje poslovnih in tehnično-tehnoloških zmožnosti (notranjih in zunanjih);
- ocena trenutne digitalne zrelosti organizacije, potrebo po spremembi in pripravljenost na spremembo, pri čemer se glede na navedeno določi ciljne izdelke in storitve ter zahtevane zmožnosti;
- nove referenčne standarde, najboljše prakse in nove tehnologije;
- vrzeli med trenutnim in ciljnim okoljem, pri čemer se upošteva razvoj nove digitalne strategije v sodelovanju z relevantnimi deležniki in opisom začrtane poti s koraki, potrebnih za doseganje ciljev in nalog;
- oceno uspešnosti trenutnih izdelkov in storitev ter razumevanje poslovnih in tehnično-tehnoloških potreb in sposobnosti.

OI posebno pozornost namenja spremljanju novosti na področju varovanja informacij in informacijske podpore. Pri tem skrbi, da se v organizaciji:

- proaktivno prepozna priložnosti za inovacije in načrtuje, kako jih izkoristiti glede na poslovne potrebe in strateške cilje organizacije;
- analizira, kakšne priložnosti za poslovne inovacije ali lahko izboljšave ustvarijo nastajajoče tehnologije;
- ustvarja okolje, ki spodbuja inovacije, pri čemer upošteva metode, kot so delovna uspešnost oz. raznovrstno nagrajevanje, sodelovanje, tehnološki forumi in mehanizmi za spodbujanje ter zajem idej uporabnikov informacijskih storitev;
- sodeluje z relevantnimi deležniki, da razume njihove izzive ter pridobi njihovo podporo;
- ima ustrezno razumevanje poslovne strategije, konkurenčnega okolja in drugih omejitev, da lahko prepozna priložnosti, omogočene z novimi tehnologijami;
- ima vzpostavljen proces spremljanja tehnologij, da sistematično spremlja in prepozna nove tehnologije, ki imajo potencial za ustvarjanje vrednosti (npr. z uresničevanjem poslovne strategije, optimizacijo stroškov, izogibanjem zastarelosti ter boljšim omogočanjem poslovnih in tehnično-tehnoloških procesov);
- spremlja trg, konkurenčno okolje, panoge ter pravne in regulativne trende, da lahko analizira nove tehnologije ali inovativne ideje v okviru organizacije;
- analizira prepoznane nove tehnologije in/ali druge inovativne predloge s predmetnega področja, da razume njihov poslovni potencial;
- spremlja izvajanje in uporabo novih tehnologij in inovacij med sprejemanjem, integracijo ter skozi celoten življenjski cikel, da zagotovi, da so obljubljene koristi uresničene ter pridobi izkušnje.

POLITIKA SPREMEMB INFORMACIJSKEGA SISTEMA

Namen:

Opis pravil za upravljanje informacijskega sistema

7.1. TERMINOLOŠKI SLOVAR

Produksijsko okolje: okolje, kjer poteka obratovanje informacijskega sistema.

Testno okolje: okolje, kjer se opravljajo testi aplikacij pred sprejemom v obratovanje.

Varnostni pregled: pregled stanja informacijskega sistema s stališča varnosti s pomočjo orodij (penetracijsko testiranje), ki preverjajo možnost zlorab informacijskega sistema.

Ocena skladnosti varstva podatkov: pregled stanja informacijske varnosti s strani Pooblaščen osebe za varstvo podatkov (DPO).

7.2. NAMEN POLITIKE ZA NADZOR SPREMEMB INFORMACIJSKEGA SISTEMA

Politika določa postopke sprememb informacijskega sistema. Neodobrene spremembe imajo lahko za posledico nedelovanje informacijskega sistema, kar lahko povzroči nezmožnost zagotavljanja storitev OI.

7.3. NABAVA PROGRAMSKE IN STROJNE OPREME

Nabava programske in strojne opreme se izvaja skladno z rednim ali izrednim letnim planom nabave. Nabavljena programska oprema mora upoštevati varnostne zahteve iz Politike razvoja, spreminjanja in vzdrževanja aplikacij.

7.4. NAMESTITEV PROGRAMSKE IN STROJNE OPREME

Programsko opremo se pred namestitvijo v produkcijsko okolje ustrezno testira v testnem okolju. Vsa programska oprema mora ustrezati licenčnim zahtevam.

Nameščati je dovoljeno le programsko in strojno opremo, ki jo potrdi vodja Sektorja za informatiko. Vsa programska in strojna oprema mora biti nameščena s strani zaposlenih Sektorja za informatiko ali pogodbenih sodelavcev, in usklajena s postopki varovanja informacij.

Uporabnike informacijskih storitev se predhodno obvesti o spremembah programske in strojne opreme, ki bi lahko povzročile spremembe pri njihovem rednem delu.

7.5. NADZOR NAD VERZIJAMI PROGRAMSKE OPREME

Vsaka spremenjena verzija programske opreme, ki se namesti v produkcijsko okolje, mora biti enolično označena, da je zagotovljena sledljivost nad verzijami. Oznako verzije programske opreme določi razvijalec programske opreme. Evidenco verzij se vodi pri razvijalcu programske opreme.

7.6. NADZOR SPREMEMB INFORMACIJSKEGA SISTEMA

Spremembe programske in strojne opreme se redno preverja, da se ugotavlja, ali so bile spremembe primerno vpeljane in zadostujejo primernemu nivoju informacijske varnosti.

OI za preverjanje skladnosti programske in strojne opreme uporablja mehanizme varnostnih pregledov. Varnostni pregled informacijskega sistema se izvaja, ko pride do sprememb programske in strojne opreme.

7.7. UPOŠTEVANJE TRENUTNIH IN BODOČIH POTREB

OI si prizadeva zagotoviti, da so informacijsko-tehnološki izdelki, storitve in raven storitev usklajeni s trenutnimi in bodočimi potrebami organizacije.

- Ključna so predvsem sledeča načela: analiza potreb organizacije: Redno se analizira trenutne in bodoče potrebe organizacije na področju informacijskih tehnologij. To vključuje oceno poslovnih ciljev, strategije rasti in razvoja ter pričakovanj deležnikov, da se lahko identificira ključne zahteve in pričakovanja;
- načrtovanje in razvoj storitev na področju informacijskih tehnologij: Na podlagi analize potreb organizacije se načrtuje in razvija ustrezne storitve; Pri tem se upošteva tako trenutne, kot tudi bodoče potrebe, da se zagotovi dolgoročno uspešno izpolnjevanje zahtev organizacije;
- spremljanje ravni storitev: Neprestano spremljanje in ocenjevanje ravni storitev na področju informacijskih tehnologij, kar vključuje preverjanje skladnosti z zahtevami, ocenjevanje zadovoljstva uporabnikov ter identifikacijo morebitnih izboljšav in prilagoditev;
- prilagajanje spremembam: Zaradi hitrih sprememb v tehnološkem okolju in poslovnih potrebah se storitve in raven storitev prilagaja glede na spremembe v okolju, da vedno ustrezajo trenutnim in bodočim potrebam organizacije;
- s stalnim prilagajanjem in izboljševanjem storitev ter ravni storitev se zagotavlja, da so informacijsko-tehnološke rešitve vedno v skladu z zahtevami in pričakovanji organizacije, kar omogoča uspešno podporo poslovnim ciljem in strategiji rasti;
- izvedba izvedljivostne študije potencialnih alternativnih rešitev, ocena njihove izvedljivosti in izbira preferirane možnosti. Po potrebi se implementira izbrano možnost kot pilotni projekt za ugotavljanje morebitnih izboljšav;
- OI izvaja sistematičen pristop k izvedljivostni študiji potencialnih alternativnih rešitev, oceni njihove izvedljivosti ter izbiro najboljše možnosti. Postopek zajema naslednje korake:
 - identifikacija potrebe po rešitvi: Prvi korak je jasna identifikacija problema ali priložnosti, ki zahteva rešitev. To lahko vključuje analizo obstoječih izzivov, upoštevanje poslovnih ciljev in pričakovanj deležnikov;
 - priprava alternativnih rešitev: Na podlagi identificirane potrebe se pripravi več alternativnih rešitev, ki bi lahko zadovoljile zahteve. Vsaka rešitev se podrobno preuči in oceni glede na njeno izvedljivost, stroške, koristi, tveganja in druge ključne dejavnike;
 - izvedljivostna študija: Vsaka alternativna rešitev se nato podvrže izvedljivostni študiji, ki oceni, ali je izvedba rešitve tehnično, finančno in operativno izvedljiva. To vključuje oceno tehnoloških zahtev, potrebnih virov, predvidenih stroškov in tveganj;
 - izbira preferirane možnosti: Na podlagi rezultatov izvedljivostne študije se izbere najboljša možnost, ki najbolje ustreza potrebam in ciljem organizacije ter hkrati zagotavlja najvišjo vrednost in najmanjše tveganje;
 - implementacija pilotnega projekta: Če je primerno, se izbrana možnost lahko implementira kot pilotni projekt, ki omogoča preizkus rešitve v realnem okolju. Med pilotnim projektom se spremljajo rezultati in identificirajo morebitne izboljšave ali prilagoditve;
 - evaluacija in iterativno izboljševanje: Po končanem pilotnem projektu se izvede celovita evalvacija, ki oceni uspešnost rešitve in identificira morebitne prilagoditve ali izboljšave. Na podlagi teh ugotovitev, se lahko izvedejo nadaljnji koraki za optimizacijo rešitve.

POLITIKA DNEVNIKOV OBDELAV / REVIZIJSKIH SLEDI

Namen: Opis pravil glede vodenja revizijskih sledi nad podatki

8.1. TERMINOLOŠKI SLOVAR

Revizijska sled: zapis vseh dejanj, ki jih uporabniki izvedejo v informacijskem sistemu, kjer se obdelujejo občutljivi podatki, kot so osebni in zdravstveni podatki. Gre za podroben zapis vseh aktivnosti, povezanih z obdelavo podatkov, in omogoča popolno sledljivost dostopov, sprememb in prenosov podatkov. Revizijska sled je namenjena zagotavljanju preglednosti, varnosti in skladnosti z zakonodajo ter omogoča kasnejše preverjanje, ali so bile vse aktivnosti izvedene zakonito in pravilno.

Dnevnik obdelave je zapis vseh aktivnosti, povezanih z obdelavo osebnih podatkov v določenem informacijskem sistemu. V dnevniku obdelave se beležijo podatki o tem, kdo, kdaj in zakaj je dostopal do osebnih podatkov, ter katere aktivnosti so bile izvedene (npr. vpogled, posodobitev, brisanje podatkov).

8.2. NAMEN POLITIKE ZA ZAGOTAVLJANJE REVIZIJSKIH SLEDI

Namen politike je zagotoviti varnost in zaupnost osebnih ter zdravstvenih podatkov pacientov. Ta politika določa pravila in postopke, ki urejajo, kdo in pod kakšnimi pogoji lahko dostopa do občutljivih podatkov, ter kako se spremljajo in beležijo vsi dostopi do teh podatkov z uporabo revizijskih sledi.

Glavni cilji te politike so:

Zaščita podatkov: Preprečiti nepooblaščen dostop do osebnih in zdravstvenih podatkov pacientov.

Sledljivost: Ustvariti sistem, ki omogoča beleženje in preverjanje vseh aktivnosti uporabnikov v informacijskih sistemih, kjer se obdelujejo občutljivi podatki.

Odgovornost: Zagotoviti, da so vsi zaposleni odgovorni za svoje aktivnosti in dostop do podatkov ter da se nepooblaščen dostop hitro odkrijejo in obravnavajo.

Zakonodajna skladnost: Zagotoviti skladnost z zakonodajo ter z notranjimi pravili bolnišnice glede varstva osebnih podatkov.

Preprečevanje zlorab: Z vzpostavitvijo revizijskih sledi se zmanjšuje možnost zlorab in nepooblaščenih dostopov, saj so vsi dostopi zabeleženi in kasneje preverljivi.

8.3. SKLADNOST IN NADZOR

Vodenje dnevnika obdelave ni samo zahteva za skladnost z nacionalno in EU zakonodajo s področja varstva osebnih podatkov, ampak služi tudi kot vitalno orodje za samonadzor v organizacijah, ki jim omogoča, da redno pregledujejo in ocenjujejo svoje postopke obdelave podatkov. To pomaga pri prepoznavanju morebitnih slabosti v varstvu podatkov in pri izvajanju potrebnih izboljšav. Dnevnik obdelave tako igra ključno vlogo pri gradnji zaupanja med organizacijami, uporabniki in regulatornimi organi z zagotavljanjem visoke stopnje preglednosti in odgovornosti v obdelavi osebnih podatkov.

8.4. ZAGOTAVLJANJE REVIZIJSKIH SLEDI

Nad informacijami, aplikacijami in informacijskimi sistemi so vzpostavljene revizijske sledi, ki omogočajo zagotavljanje sledljivosti naslednjih dogodkov:

- obdelav osebnih podatkov in občutljivih osebnih podatkov ter poslovne skrivnosti,
- aktivnosti uporabnikov storitev.

Glavni namen dnevnika obdelave je zagotoviti jasen in natančen zapis o tem, kdo, kdaj, kako in zakaj obdeluje osebne podatke. To vključuje informacije o vrstah zbranih podatkov, namenu obdelave, uporabnikih sistema in zunanjih pooblaščenih osebah, ki so jim podatki bili razkriti, ter predvidenih rokih za izbris podatkov. Dnevnik prav tako služi kot orodje za analizo in revizijo procesov obdelave podatkov, omogoča identifikacijo in odpravljanje varnostnih tveganj, ter pripomore k izboljšanju politik in praks varstva podatkov.

Zaradi zagotavljanja učinkovitosti in skladnosti z zakonodajo mora dnevnik obdelave vsebovati:

- **Ime ali ID številka uporabnika:** Dnevnik beležijo identiteto zaposlenega, ki je dostopal do podatkov.
- **Datum in čas dostopa:** Natančen čas, ko je bil dostop opravljen, kar omogoča določitev, kdaj je prišlo do vpogleda ali obdelave podatkov.
- **Vrsta dostopa:** Beleženje, ali je šlo za ogled, posodabljanje, prenos ali izbris podatkov. To pomaga ugotoviti, kakšna obdelava je bila izvedena.
- **Namen dostopa:** V bolnišničnem okolju mora biti dostop do osebnih podatkov vedno povezan s specifičnim namenom, kot je zdravstvena obravnava, priprava terapije, diagnostični pregledi, ali druga nujna obravnava pacienta.
- **Specifični podatki o pacientu:** Kateri podatki so bili obdelani (npr. zdravstvena kartoteka določenega pacienta, laboratorijski izvidi, diagnostične slike).

Dnevnik obdelave se štiti pred nepooblaščenim dostopom in spreminjanjem.

V skladu z Zakonom o varstvu podatkov morajo biti dnevniki obdelave v bolnišnici hranjeni najmanj 5 let po zadnjem dostopu, razen če zakonodaja zahteva daljše obdobje (npr. pri sodnih postopkih ali pri podatkih, povezanih z dolgoročno zdravstveno oskrbo). To omogoča, da se morebitne nepravilnosti odkrijejo tudi več let po dostopu.

8.5. SLEDLJIVOST OBDELAV OSEBNIH PODATKOV, OBČUTLJIVIH OSEBNIH PODATKOV IN POSLOVNE SKRIVNOSTI

Sledljivost obdelav podatkov mora biti primerna obdelovanim podatkom in se uporablja za vse osebne podatke, občutljive osebne podatke in poslovno skrivnost.

8.5.1. Osebni podatki in poslovna skrivnost

Prvi nivo sledljivosti velja za osebne podatke in poslovno skrivnost, kjer je omogočeno naknadno ugotavljanje, kdo je vnesel, spremenil ali izbrisal kateri podatek in kdaj. Informacijski sistem OI zagotavlja beleženje aktivnosti uporabnikov informacijskih storitev, ki vključuje vpis, spremembo in izbris posameznega osebnega podatka ali poslovne skrivnosti. Revizijske sledi nad osebnimi podatki v papirni dokumentaciji se beležijo z evidenco dostopov do papirne dokumentacije.

8.5.2. Občutljivi varovani osebni podatki

Drugi nivo sledljivosti velja za občutljive osebne podatke, kjer je omogočeno naknadno ugotavljanje, kdo je vnesel, spremenil ali izbrisal kakšen podatek in kdaj, poleg tega pa se beleži tudi, kdo in kdaj je do določenega podatka zgolj dostopil (vpogled, seznanitev), a podatka ni spremenil. Informacijski sistem OI zagotavlja beleženje aktivnosti uporabnika, ki vključujejo vpis, spremembo in izbris ter dostop (vpogled) do posameznega občutljivega osebnega podatka. Revizijske sledi nad občutljivimi osebnimi podatki v papirni dokumentaciji se beležijo z evidenco dostopov do papirne dokumentacije.

8.6. SLEDLJIVOST AKTIVNOSTI UPORABNIKOV INFORMACIJSKIH STORITEV Z ADMINISTRATIVNIMI RAČUNI

Pogodbени sodelavci zagotavljajo revizijsko sled nad dostopi do informacijskih sistemov uporabnikov informacijskih storitev (tudi svojih), ki imajo administratorske račune.

8.7. DOSTOP DO HRAMBE PODATKOV O DOSTOPIH (VPOGLEDIH)

Podatki o dostopih (vpogledih) so v informacijskem sistemu OI in v evidenci dostopov do papirne dokumentacije. Do dnevnikov obdelave imajo dostop le pooblašcene osebe, kot so Skrbnik SUVI, pooblašcana oseba za varstvo osebnih podatkov, vodje informacijske varnosti ali drugi odgovorni za zagotavljanje skladnosti z zakoni.

8.8. NADZOR

V primeru nepooblaščenega dostopa ali suma na nepooblaščen dostop, se ravna v skladu s Politiko o varnostnih incidentih. V primeru incidentov, ki lahko povzročijo ali so povzročili izgubo, uničenje ali zlorabo osebnih podatkov, občutljivih osebnih podatkov ali zaupnih podatkov, je treba takoj izvesti ukrepe za zaščito teh podatkov in preprečitev nadaljnje škode. Postopek obravnave vključuje naslednje korake:

POLITIKA UPORABE STORITEV INTERNETA

Namen:

Opis pravil za dostop do elektronske pošte in svetovnega spleta

9.1. TERMINOLOŠKI SLOVAR

Elektronska pošta: izmenjava sporočil v elektronski obliki z uporabo protokola SMTP.

Internet: globalno omrežje računalnikov in omrežij, ki se razprostira preko vsega sveta.

Svetovni splet: storitve, dosegljive po računalniškem informacijskem sistemu preko omrežja internet.

9.2. NAMEN POLITIKE ZA UPORABO STORITEV INTERNETA

Politika opredeljuje pravila varne uporabe storitev interneta (svetovnega spleta, elektronske pošte). Z izvajanjem postopkov varne rabe informacij in informacijskega sistema se zmanjša možnost razkritja, nepooblaščne spremembe in izgube podatkov, možnost okužbe z zlonamerno programsko opremo in prepreči izpad storitev interneta.

9.3. UPORABA STORITEV INTERNETA

Internetna povezava OI (z izjemo brezžične povezave onko-public) je namenjena službeni uporabi.

9.4. UPORABA SVETOVNEGA SPLETA (WWW)

Uporabniki informacijskih storitev lahko dostopajo do svetovnega spleta preko ponudnika internetnih storitev OI.

Uporabnikom informacijskih storitev ni dovoljeno:

- širjenje ali dostopanje do žaljivih in nezakonitih vsebin na svetovnem spletu,
- nalaganje datotek iz nezanesljivih oziroma sumljivih spletnih strani,
- prenašanje programske opreme v nasprotju z licenčnimi pogoji,
- nezakonito kopiranje in izraba avtorskih izdelkov.

9.5. OMEJEVANJE DOSTOPA DO SVETOVNEGA SPLETA

Dostopanje do določenih naslovov ali določenih vsebin se omeji. Direktor na predlog vodje Sektorja za informatiko določa naslove ali vsebine, do katerih se bo tehnično omejil dostop.

9.6. POLITIKA UPORABE ELEKTRONSKE POŠTE

Elektronska pošta OI je namenjena službeni uporabi.

Uporabniki storitev smejo za službeno elektronsko pošto uporabljati le naslove elektronske pošte OI.

Uporabniki storitev smejo uporabljati poštne predale, za katere so pooblaščen in ne smejo omogočiti uporabe poštne predala nepooblaščenim osebam.

Elektronsko pošto in priponke, ki vsebujejo občutljive osebne podatke je potrebno pri pošiljanju v zunanje omrežje (prejemnikom izven OI) kriptirati in elektronsko podpisati. Podatki se pošiljajo skladno z dokumentom Navodila za varno pošiljanje osebnih podatkov.

Pri pošiljanju, posredovanju ali vračanju elektronske pošte (forward, reply) morajo biti uporabniki informacijskih storitev še posebej previdni in preveriti ali je pošta naslovljena na prave naslove.

Uporabnik storitev mora previdno ravnati z elektronsko pošto in priponkami neznanega oziroma sumljivega pošiljatelja. Tovrstne elektronske pošte in priponk se ne odpira, ampak izbriše. Če je pošiljatelj znan, sumljiv pa je naslov ali vsebina elektronske pošte, mora uporabnik storitev pri pošiljatelju ali sektorju za informatiko preveriti izvor elektronske pošte.

Uporabniki informacijskih storitev ne smejo uporabljati sistema elektronske pošte za:

- sodelovanje v verižni pošti,
- širjenje zlonamerne programske opreme,
- širjenje žaljivih in nezakonitih vsebin, avtorsko zaščitene informacij in računalniških programov v nasprotju z licenčnimi pogoji,
- pošiljanje velike količine elektronske pošte (spam) ali priponk z vsebino, ki ni povezana z opravljanjem delovnih nalog,
- preusmeritev elektronske pošte na drug poštni predal izven omrežja Inštituta.

Uporabnik storitev mora nemudoma obvestiti Sektor za informatiko v primeru, ko:

- protivirusna programska oprema odkrije škodljivo kodo,
- uporabnik sumi, da je elektronska pošta okužena z virusom,
- sporočilo vsebuje povezavo z zahtevo za spremembo gesla,
- sporočilo zahteva od uporabnika vnos osebnih ali drugih občutljivih podatkov
- uporabnik sumi na zlorabo domenskega uporabniškega računa ali vdor v informacijski sistem.

Ob prenehanju delovnega razmerja ali prenehanju avtorske ali podjetne pogodbe, se dostop do elektronske pošte ukine. Vsebina poštnega predala se po potrebi, na podlagi pisnega naročila Kadrovske službe Sektorju za informatiko, arhivira za zahtevano časovno obdobje.

Na prošnjo uporabnika se na podlagi pisnega naročila Kadrovske službe Sektorju za informatiko za obdobje 1 meseca lahko aktivira odzivnik o ukinitvi elektronskega naslova.

Uporabniku se omogoči, da morebitno zasebno pošto odstrani ali shrani na drug podatkovni medij. Do prenehanja delovnega razmerja ali prenehanja avtorske ali podjetne pogodbe je uporabnik dolžan pregledati svoj poštni predal, predati za delo pomembne informacije sodelavcem in izbrisati občutljive podatke.

Uporabnik mora elektronska sporočila, ki jih ne potrebuje več, občasno brisati iz svojega poštnega predala, oziroma mora to storiti na zahtevo Sektorja za informatiko.

9.7. OMEJEVANJE UPORABE ELEKTRONSKE POŠTE

Pošiljanje in sprejemanje priponk določenega formata lahko Sektor za informatiko onemogoči z namenom zmanjšanja možnosti okužbe z zlonamerno programske opreme (neposredno izvršljive datoteke s končnicami .exe, .bat, .pif itd.).

Dovoljena največja velikost priponke je omejena glede na razpoložljive računalniške vire in potrebe delovnega mesta uporabnika.

9.8. NADZOR UPORABE STORITEV INTERNETA

Informacijski sistem OI beleži podatke o prometu v in iz interneta, ter podatke o dogodkih, povezanih z uporabo in upravljanjem sistema elektronske pošte.

V primeru zaznanih varnostnih incidentov, Skrbnik SUVI opravi nadzor v skladu s Politiko upravljanja varnostnih incidentov.

POLITIKA UPRAVLJANJA IN VAROVANJA GESEL

Namen: Opis zahtev upravljanja z gesli za dostop do informacij, aplikacij in informacijskih sistemov

10.1. TERMINOLOŠKI SLOVAR

Uporabniško ime: ime, ki se določi zaposlenemu ali pogodbenemu sodelavcu za dostop do informacij, aplikacij in informacijskih sistemov.

Skupinska uporabniška imena in gesla: uporabniška imena in gesla, ki jih uporablja več uporabnikov informacijskih storitev OI.

Gesla administratorskega računa: gesla skrbnika aplikacije ali informacijskega sistema.

10.2. NAMEN POLITIKE UPRAVLJANJA IN VAROVANJA GESEL

Namen politike je predpisati obveznosti in pravila za varno ravnanje z gesli, redno menjavo na 6 mesecev in izbiro kakovostnih gesel z namenom zmanjševanja tveganja zlorabe gesel, nepooblaščenega dostopa, ogrožanja ali kraje informacij.

10.3. VARNO RAVNANJE Z GESLI

Uporabniško ime in geslo je namenjeno posameznemu uporabniku informacijskih storitev.

Po prejemu uporabniškega imena in gesla s strani Sektorja za informatiko je uporabnik storitev dolžan varovati svoje geslo in ga ne sme razkrivati drugim osebam.

Začasno geslo mora uporabnik spremeniti ob prvi prijavi.

Gesla se ne smejo zapisovati ali shranjevati na način, ki bi nepooblašчени osebi lahko omogočil dostop do gesla.

Če uporabnik informacijskih storitev zasledi malomarno ali zlonamerno ravnanje z gesli, mora to takoj sporočiti Sektorju za informatiko ali Skrbniku SUVI. Geslo mora uporabnik storitev spremeniti takoj, če obstaja sum na razkritje gesla, in o tem obvestiti Sektor za informatiko ali Skrbnika SUVI.

Skupinska uporabniška imena in gesla se lahko uporabljajo izključno v kolikor se z njimi ne more dostopati do osebnih podatkov ali občutljivih osebnih podatkov.

V kolikor je geslo uporabljeno za nepooblaščen dostop do informacij, aplikacij ali informacijskih sistemov OI se vodi postopek skladno s Politiko upravljanja varnostnih incidentov.

10.4. REDNA MENJAVA IN IZBIRA KAKOVOSTNEGA GEsla

Pri izbiri gesel so uporabniki informacijskih storitev dolžni upoštevati naslednja pravila:

- izbirati je potrebno gesla z najmanj 16 znaki,

Priporoča se, da:

- je geslo kompleksno (uporaba velikih in malih črk, števil in posebnih znakov, najmanj 16 mest);
- naj geslo ne vsebuje šumnikov;
- geslo združuje tri ali štiri slovenske besede (npr. najvednosijesonce);
- geslo vsebuje pomensko področje kot so slovenske pesmi ali različni športi (npr. mediskrenimiljudmi, tobodotrijeprostiteti).
- da geslo ne vsebuje angleških, nemških, španskih in ruskih besed;
- uporabo pogovornega jezika ali slenga.

10.5. DODATNA PRAVILA ZA IZBIRO GESEL IN HRAMBA GESEL ZA ADMINISTRATORSKE RAČUNE

Pri izbiri in menjavi gesel za administratorske račune so zaposleni Sektorja za informatiko in pogodbeni sodelavci dolžni upoštevati še naslednja pravila:

- administratorska gesla imajo vsaj 16 znakov.

Vsa gesla administratorskih računov aplikacij in informacijskih sistemov je potrebno shraniti v varovanem območju prostorov upravne dejavnosti (blagajne, omare), da se v nujnih primerih zagotovi možnost dostopa do aplikacij in informacijskih sistemov tudi v odsotnosti posameznih administratorjev (zaposlenih Sektorja za informatiko ali pogodbenih sodelavcev). Vsa gesla administratorskih računov so hranjena na način, da je onemogočen dostop nepooblaščenim osebam.

Uporaba gesla administratorskega računa v primeru nujnega posega se mora zabeležiti v evidenčni list. Zapisati je potrebno osebo, ki je dostopala do gesla, datum in čas uporabe gesla. Geslo morajo zaposleni Sektorja za informatiko v najkrajšem možnem času spremeniti.

10.6. IZBIRA IN MENJAVA GESEL KONTROLE FIZIČNEGA DOSTOPA (ALARMNI SISTEM)

Pri izbiri in menjavi gesel so uporabniki dolžni upoštevati naslednja pravila:

- vsak uporabnik ima svoje geslo,
- geslo se v primeru prekinitve delovnega razmerja izbriše iz sistema.

10.7. NEUPRAVIČENO RAVNANJE Z GESLOM OZIROMA UPORABNIŠKIM IMENOM

Vsak zaposleni OI ali pogodbeni sodelavec je dolžan uporabljati geslo ali uporabniško ime, ki mu je dodeljeno, v skladu s sprejeto politiko varovanja informacij. Zaposleni OI ali pogodbeni sodelavec sme uporabljati dodeljeno geslo ali uporabniško ime v svojem imenu in v skladu s pooblastili, ki so mu podeljena s pogodbo o zaposlitvi oziroma drugim pooblastilom, vezanim na razmerje pri delodajalcu.

Zaposleni OI ali pogodbeni sodelavec mora posebej skrbno varovati svoje osebno geslo oziroma uporabniško ime in jih ne sme dajati v uporabo ali na vpogled drugim nepooblaščenim osebam. Za kršitev te obveznosti odškodninsko odgovarja v skladu z Zakonom o delovnih razmerjih in splošnimi pravili civilnega prava. Ravnanje, ki je v nasprotju s sprejeto politiko varovanja informacij, se smatra za hujšo kršitev delovnega razmerja oz. pogodbenih obveznosti.

10.8. NADZOR NAD UPRAVLJANJEM Z GESLI

Skrbnik SUVI periodično (najmanj dva krat letno) preverja in evidentira ali je upravljanje z gesli skladno s tem navodilom. V primeru zaznanega neustreznega ravnanja sproži postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA VAROVANJA V POVEZAVI Z ZAPOSLENIMI

Namen:

Opis pravil v SUVI za zaposlene OI

11.1. TERMINOLOŠKI SLOVAR

Dokumentacija varnostnih politik: vsi dokumenti, ki določajo postopke primerne uporabe informacij in informacijskih sredstev.

Sredstva informacijskega sistema: vsa računalniška sredstva in nosilci podatkov, kjer se nahajajo osebni podatki, občutljivi osebni podatki ter poslovna skrivnost.

11.2. NAMEN POLITIKE VAROVANJA V ZVEZI Z ZAPOSLENIMI

Politika določa, kakšni so ustrezni postopki pri zaposlovanju in vodenju ukrepov, ki so povezani z zaposlenimi OI glede izobraževanja, usposabljanja in preverjanja, splošnih postopkov varovanja informacij OI ter odgovornosti zaposlenih.

Vse določbe te politike veljajo skladno z vsebino obveznih internih aktov OI, ter Kodeksa ravnanja delavcev OI.

11.3. IZOBRAŽEVANJE, USPOSABLJANJE IN PREVERJANJE

Za izobraževanje zaposlenih glede določil sistema za upravljanje varovanja informacij je zadolžen Skrbnik SUVI.

Izobraževanje se opravlja ob prihodu novega zaposlenega ter vsaj 1-krat na 3 leta za vse zaposlene oziroma takrat, ko je to potrebno zaradi sprememb politike varovanja informacij, postopkov ali navodil. O izobraževanjih se vodi evidence, ki jih hrani Skrbnik SUVI.

11.4. VAROVANJE INFORMACIJ NA OI

Ustrezno varovanje informacij se začne že pred samo zaposlitvijo, traja ves čas zaposlitve in se mora zagotavljati tudi po preteku zaposlitve na OI.

11.5. POSTOPKI PRED ZAPOSLOTVIJO

Pred zaposlitvijo Kadrovska služba OI novo zaposlenega seznani z dokumentacijo varnostnih politik, ki jih mora upoštevati.

V pogodbi o zaposlitvi so jasno opredeljena načela varovanja informacij oziroma je podan sklic na dokumentacijo sistema za upravljanje varovanja informacij in sankcije v primeru izgube, uničenja ali zlorabe informacij.

11.6. POSTOPKI MED ZAPOSLOTVIJO

Skrbnik SUVI preverja ali zaposleni upoštevajo vsa določila dokumentacije sistema za upravljanje varovanja informacij in v primeru neupoštevanja sprejema ustrezne ukrepe skladno s Politiko upravljanja incidentov. Vse spremembe, ki vplivajo na varovanje informacij, morajo biti posredovane vsem zaposlenim OI.

11.7. POSTOPKI OB PREKINITVI ZAPOSLOTVE

Vsi zaposleni morajo ob koncu zaposlitve vrniti vsa sredstva informacijskega sistema OI, ki so jih prejeli v uporabo. Vsem zaposlenim se ob koncu zaposlitve odvzame pravice fizičnega in računalniškega dostopa do informacij in informacijskega sistema. Odgovornosti in obveznosti glede varovanja informacij, ki veljajo tudi po koncu zaposlitve, so vključene v pogodbe o zaposlitvi.

11.8. ODGOVORNOST ZAPOSLENIH OI

Za izvajanje primernih varnostnih ukrepov so zadolženi zaposleni, Skrbnik SUVI OI pa je odgovoren za izvajanje mehanizmov varovanja informacij v celoti in za zagotovitev potrebnih virov, ki omogočajo primerno vodenje sistema za upravljanje varovanja informacij.

POLITIKA UPRAVLJANJA KAKOVOSTI IN VARNOSTI STORITEV POGODBENIH SODELAVCEV

Namen:

Opis pravil v SUVI za pogodbene sodelavce

12.1. TERMINOLOŠKI SLOVAR

Neprekinjenost storitev: storitve, ki delujejo glede na poslovne potrebe brez neželenih prekinitev.

Pogodbeni sodelavci: partnerji ali pogodbeni sodelavci, ki izvajajo storitve za OI.

12.2. NAMEN POLITIKE ZA UPRAVLJANJE KAKOVOSTI IN VARNOSTI POGODBENIH SODELAVCEV

Politika predstavlja postopke upravljanje kakovosti in varnosti storitev pogodbenih sodelavcev, s katerimi OI zagotovi, da pogodbeni sodelavci izvajajo dogovorjeno raven storitev in zagotavljajo ustrezno varnost informacij.

12.3. POGODBENO UREJANJE RAZMERIJ S POGODBENIMI SODELAVCI

Pogodba o sodelovanju opredeljuje opis storitev in predvideni rok trajanja opravljanja teh storitev pogodbenih sodelavcev v skladu z zakonodajo, ki ureja varstvo osebnih podatkov.

Določila o seznanjenosti s postopki varovanja informacij za pogodbene sodelavce, se vključi v pogodbo o sodelovanju, ali doda kot samostojno prilogo k pogodbi.

Določila pogodbene sodelavce obvezujejo, da izvajajo postopke varovanja informacij, ki preprečujejo:

- izgubo, uničenje ali zlorabo osebnih podatkov, občutljivih osebnih podatkov ter poslovne skrivnosti,
- poškodovanje ali zlorabo informacijskega sistema,
- krajo programske ali strojne opreme,
- izpad delovanja informacijskega sistema (strojna oprema, programska oprema, komunikacije),
- kršenje zakonodaje,
- neupoštevanje postopkov varovanja informacij.

Pri tem se skladno s pogodbo o sodelovanju izvajajo postopki varovanja informacij skozi celotno obdobje sodelovanja in po zaključku sodelovanja s pogodbenimi sodelavci.

V pogodbo s pogodbenimi sodelavci se vključi tudi določila o:

- načinu poročanja ter obveščanja o varnostnih incidentih,
- vodenje in dostopnost seznama vseh oseb pogodbenih sodelavcev, pooblaščenih za izvajanje storitev na OI,
- načinu zagotavljanja, da se vse osebe, ki so povezane s pogodbenim sodelovanjem, vključno s podizvajalci, zavedajo svojih obveznosti glede postopkov varovanja informacij OI.

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

Kjer je neprekinjeno delovanje storitev pogodbenih sodelavcev nujno za izvajanje poslovnih procesov OI, se pri naročanju storitev dogovori o ustrezni ravni storitev, ki se morajo ohraniti tudi v primeru nepredvidenih dogodkov, npr. pri večjih okvarah ali nesrečah.

Pred sklenitvijo pogodbe oziroma pred izvajanjem storitev morajo vse osebe pogodbenih sodelavcev, ki izvajajo dela po pogodbi, podpisati ustrezno izjavo o seznanitvi in sprejemanju varnostnih zahtev, ki jih določajo postopki varovanja informacij, katere določa Krovna politika varovanja informacij in Sporazum o obdelavi osebnih podatkov na OIL.

12.4. UPRAVLJANJE SPREMEMB STORITEV POGODBENIH SODELAVCEV

Spremembe pri zagotavljanju storitev pogodbenih sodelavcev upravljajo skrbniki pogodbenih sodelavcev oziroma Skrbnik SUVI, ki najmanj enkrat letno preverja pogodbe s pogodbenimi sodelavci. Skrbnik SUVI je odgovoren za:

- informiranje pogodbenih sodelavcev o novih določbah postopkov varovanja informacij,
- nadzor in spremljanje izvajanja storitev in upoštevanja postopkov varovanja informacij,
- spremljanje sprememb pri izvajanju storitev in po potrebi sprožitev postopka za spremembo postopkov varovanja informacij in pogodb s pogodbenimi sodelavci.

12.5. NADZOR POGODBENIH SODELAVCEV

Pogodbenim sodelavcem zaposleni Sektorja za informatiko omogočijo dostop samo do tistih informacij, aplikacij in informacijskih sistemov, ki jih nujno potrebujejo pri zagotavljanju storitev.

V primeru zaznanega incidenta, Skrbnik SUVI sproži postopke skladno s Politiko upravljanja varnostnih incidentov.

12.6. NABAVA NAPRAV ALI STORITEV TER SODELOVANJE Z DOBAVITELJI OZ. ZUNANJIMI IZVAJALCI

Vsaka večja nabava naprav in storitev se začne z oblikovanjem in potrditvijo pisne uporabniške zahteve s strani odgovornega skrbnika. Na podlagi uporabniške zahteve se preverijo zahteve glede na obstoječo infrastrukturo in pridobijo ponudbe dobaviteljev oziroma zunanjih izvajalcev. Izbira najugodnejše ponudbe ter načrt izvedbe odobri vodja. Izbranemu dobavitelju oz. zunanjemu izvajalcu se zagotavlja zadosten poslovni, varnostni in tehnološki nadzor. Skladno z načrtom in sklenjeno pogodbo z dobaviteljem ali zunanjim izvajalcem se nabavni ali soroden proces vedno zaključi s formalnim prevzemnim postopkom. Postopek prevzema se opravi s prevzemnim zapisnikom po uspešno opravljenih funkcijskih preizkusih in poskusnem obratovanju. Morebitne zamude ali odstopanja se zapisniško ugotovijo in skladno z načrtom in pogodbo odredijo potrebni poslovni (npr. pisno opozorilo, pogodbeni kazni) ali izvedbeni ukrepi (npr. zamenjava opreme, popravki, dopolnitve, ponoven preizkus in prevzem).

POLITIKA ZAŠČITE DELOVANJA INFORMACIJSKEGA SISTEMA

Namen: Opis zahtev podporne infrastrukture za delovanje informacijskega sistema

13.1. TERMINOLOŠKI SLOVAR

Podporna infrastruktura: sredstva, ki zagotavljajo ustrezno delovanje opreme informacijskega sistema.

Informacije in informacijski sistem OI: vsa dokumentacija in celoten računalniški informacijski sistem, kjer se nahajajo vse informacije, s katerimi zaposleni OI izvajajo svoje delo.

Brezprekinitveno napajanje: naprava, ki v primeru izpada električnega toka, poskrbi za delovanje informacijskega sistema (UPS), ki je vezana tudi na agregat.

Prenapetostna zaščita: naprava, ki v primeru previsoke električne napetosti zaščiti sredstva, katera so priključena v električno omrežje.

13.2. NAMEN POLITIKE ZA ZAŠČITO INFORMACIJSKIH SISTEMOV

Politika za zaščito informacijskih sistemov določa potrebno podporno infrastrukturo informacijskega sistema, ki zagotavlja primerno razpoložljivost informacij in informacijskega sistema za vse zaposlene in pogodbene sodelavce.

13.3. INFRASTRUKTURA

OI svoj informacijski sistem varujejo s primernimi ukrepi glede na območje, kjer se informacijski sistem nahaja.

Območja stopnje varovanja so opisana v dokumentu Dostop do prostorov na OI.

13.4. ZAGOTAVLJANJE KAKOVOSTI INFRASTRUKTURE

Vsa podporna infrastruktura (električna energija, hlajenje, komunikacijske povezave) je v primernem časovnem intervalu pregledana s strani Skrbnika SUVI, ki po potrebi angažira ustrezne strokovnjake. Pregled kakovosti infrastrukture izvaja Pooblaščen oseba za varstvo podatkov v okviru Varnostnega pregleda najmanj 1-krat letno. Skrbnik SUVI je v primeru zaznanih incidentov dolžna preverjati ustrezno kakovost podporne infrastrukture. V primeru zaznanega incidenta mora Skrbnik SUVI sprožiti postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO

Namen: Opis pravil glede zaščite proti virusom in drugi zlonamerni programski opremi

14.1. TERMINOLOŠKI SLOVAR

Zlonamerna programska oprema: programska koda z namenom škodovanja informacijskim sistemom.

Programska oprema za zaščito pred virusi in drugo zlonamerno programsko opremo: protivirusni program.

14.2. NAMEN POLITIKE ZAŠČITE PRED ZLONAMERNO PROGRAMSKO KODO

Namen dokumenta je opredeliti mehanizme za zaščito pred zlonamerno programsko opremo in zmanjšati možnost, da bi le-ta ogrozila zaupnost, celovitost ali razpoložljivost informacij, aplikacij in informacijskih sistemov.

14.3. ZAŠČITA PRED ZLONAMERNO PROGRAMSKO OPREMO

Da bi informacijski sistem OI ustrezno zaščitili pred zlonamerno programsko opremo in njenim nenadzorovanim razširjanjem se uporablja naslednje mehanizme:

- programsko opremo za zaščito pred virusi in drugo zlonamerno programsko opremo (spyware, adware, grayware itd.). Omenjena programska oprema je nameščena na vse odjemalce (delovne postaje, strežniško infrastrukturo),
- uporabljena programska oprema za zaščito pred virusi in drugo zlonamerno programsko opremo se redno posodablja, prav tako pa se redno izvaja pregledovanje nosilcev podatkov (trdih diskov in prenosnih medijev),
- segmentacija omrežja (ločevanje posameznih delov omrežja – strežniška infrastruktura, delovne postaje),
- požarni zid.

Zaposleni Sektorja za informatiko v primeru zaznanih incidentov skupaj s pogodbenimi sodelavci preverja prisotnost zlonamerne programske opreme v informacijskem sistemu OI. V primeru zaznanega incidenta mora uporabnik sprožiti postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA IZDELAVE IN SHRANJEVANJA VARNOSTNIH KOPIJ

Namen:

Opis pravil za varnostno kopiranje podatkov

15.1. TERMINOLOŠKI SLOVAR

Oddaljena lokacija: lokacija organizacije, ki je drugje kot lokacija, kjer se nahaja centralni računalniški sistem.

Ponovna vzpostavitev informacijskega sistema: postavitve informacijskega sistema po nesreči ali napaki.

Restavriranje podatkov: ponovna vzpostavitev podatkov iz npr. varnostnih kopij.

Varnostno kopiranje: kopiranje podatkov z namenom hrambe na več medijih.

15.2. NAMEN DELOVNEGA NAVODILA ZA IZDELAVO IN SHRANJEVANJE VARNOSTNIH KOPIJ

Namen izdelave in shranjevanja varnostnih kopij je zagotoviti rezervno kopijo osebnih podatkov, občutljivih osebnih podatkov, poslovne skrivnosti ter javnih podatkov in omogočiti ponovno vzpostavitev informacijskega sistema in uspešno nadaljevanje dela po dogodkih oziroma varnostnih incidentih, ki povzročijo izgubo podatkov ali nedelovanje informacijskega sistema OI – problemi s strojno opremo, problemi s programsko opremo, človeške napake, naravne nesreče ipd.

15.3. IZDELAVA VARNOSTNIH KOPIJ PODATKOV NA STREŽNIKIH

Pogostost izdelave varnostnih kopij ustreza varnostnim zahtevam poslovnih procesov OI, kar pomeni varnostno kopiranje vsak dan. Za varnostno kopiranje se uporablja prenos podatkov v elektronski obliki na oddaljeno lokacijo.

Varnostne kopije so ustrezno označene, da jih je možno v čim krajšem času in pravilno uporabiti pri restavriranju podatkov.

15.4. SHRANJEVANJE VARNOSTNIH KOPIJ

Varnostne kopije podatkov v kriptirani obliki se hranijo na oddaljeni lokaciji, do podatkov lahko dostopajo samo zaposleni Sektorja za informatiko in pogodbeni sodelavci – skrbniki sistema.

15.5. PREVERJANJE VARNOSTNIH KOPIJ

Pogodbeni skrbnik sistema 1x letno preveri, da se podatki dejansko nahajajo na oddaljeni lokaciji in da podatki niso poškodovani ali uničeni ter testira, ali bi bilo v primeru dogodka ali varnostnega incidenta podatke mogoče restavrirati iz varnostnih kopij. V ta namen se izvede popolno restavriranje naključno izbranega dela varnostne kopije v testno okolje. O restavriranju varnostnih kopij se napravi zapisnik. Zapisnik o restavriranju varnostnih kopij se posreduje Skrbniku SUVI.

15.6. NADZOR IZVAJANJA IN SHRANJEVANJA VARNOSTNIH KOPIJ

Izvajanje določil, navedenih v tem navodilu, pregleduje Skrbnik SUVI. V primeru zaznanih incidentov dostopa do varnostnih kopij in pregleda o ustreznosti zapisov varnostnih kopij ter sproži postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA IZDELAVE IN SHRANJEVANJA ARHIVSKIH DOKUMENTOV

Namen:

Opis pravil za hrambo podatkov

16.1. TERMINOLOŠKI SLOVAR

Hramba: hramba podatkov za namene kasnejše rabe.

Klasifikacijski načrt: decimalni načrt vrst gradiva in zahtev za njihovo hrambo.

Evidenca obdelav: evidenca vrste in namenov obdelav osebnih podatkov.

16.2. NAMEN POLITIKE ZA IZDELAVO IN SHRANJEVANJE DOKUMENTOV

Politika za izdelavo in shranjevanje dokumentov določa pravila in postopke arhiviranja osebnih podatkov, občutljivih osebnih podatkov ter poslovne skrivnosti.

16.3. IZDELAVA IN HRAMBA DOKUMENTOV

OI hrani osebne podatke in občutljive osebne podatke, poslovno skrivnost ter javne podatke skladno z veljavnimi predpisi.

OI hrani osebne podatke in občutljive osebne podatke, poslovno skrivnost ter javne podatke v obliki papirnih izvodov in/ ali elektronskih izvodov. Dokumenti se hranijo skladno s Politiko fizične zaščite in fizičnega dostopa.

16.4. IZDELAVA IN HRAMBA DOKUMENTOV V PAPIRNI OBLIKI

Pooblaščen osebe OI za posamezne zbirke osebnih podatkov poskrbijo za primerno hrambo dokumentov, da ne pride do poškodb ali uničenja dokumentacije oziroma zlorabe podatkov. Papirna oblika dokumentov se hrani v prostorih OI in na ustreznih zunanjih lokacijah.

16.5. IZDELAVA IN HRAMBA DOKUMENTOV V ELEKTRONSKI OBLIKI

Za hrambo zdravstvene dokumentacije v elektronski obliki je potrebno zagotoviti primerne postopke elektronske hrambe (notranja pravila, zajem, pretvorba, pogoji pretvorbe in elektronske hrambe, usklajenost s tehnološkimi standardi) ter infrastrukturo (strojna in programska oprema, ponudniki opreme in storitev, registracija, akreditacija, nadzor) skladno z zakonodajo.

Oblika zapisa se kriptira, če se hrani osebne podatke ali občutljive osebne podatke. Oblika zapisa mora zagotavljati ohranitev vsebine gradiva ter omogočati po obdobju 5 let pretvorbo v novo elektronsko obliko zapisa, ki bo takrat izpolnjevala pogoje varne hrambe gradiva. Nosilec podatkov mora zagotavljati vse pogoje varne hrambe gradiva in omogočati večje število prepisov s sedanjih na bodoče nosilce podatkov.

Elektronska oblika dokumentov se hrani v območju računalniškega informacijskega sistema in komunikacijskega sistema OI.

POLITIKA UPRAVLJANJA Z VARNOSTNIMI INCIDENTI

Namen:

Opis postopkov v primeru pojava incidenta

17.1. TERMINOLOŠKI SLOVAR

Evidenca incidentov: mesto, kjer se nahajajo zapisi vseh zaznanih incidentov.

17.2. NAMEN POLITIKE ZA UPRAVLJANJE VARNOSTNIH INCIDENTOV

Vsi zaposleni in pogodbeni sodelavci so odgovorni za ustrezno upravljanje z incidenti. To vključuje obvladovanje incidentov, odpravo oziroma zmanjšanje posledic incidentov pri izvajanju delovnih aktivnosti ter beleženje incidentov in poročanje o incidentih Skrbniku SUVI OI V primerih, ko incident vključuje osebne podatke, mora biti poleg Skrbnika SUVI o tem obveščena tudi pooblaščen oseba za varstvo osebnih podatkov (DPO), ki oceni vpliv incidenta na varstvo podatkov ter poda priporočila za nadaljne ukrepe Komisije ter Skrbnika SUVI. Incidente je potrebno skladno s postopki varovanja informacij identificirati in reševati glede na kritičnost posameznega incidenta.

Namen politike je opredeliti postopke, s katerimi se zagotovi obvladovanje oziroma odprava ali zmanjšanje posledic incidenta.

17.3. DEFINICIJA INCIDENTA

Incident predstavlja en ali več nezaželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo lahko ogrozili normalno delovanje poslovnih procesov OI oziroma zaupnost, celovitost ali razpoložljivost informacij, aplikacij ali informacijskega sistema.

Incidenti so:

- izguba, uničenje ali zloraba osebnih podatkov, občutljivih osebnih podatkov in poslovne skrivnosti (podatki v elektronski obliki, papirni dokumenti itd.),
- poškodovanje ali zloraba informacijskega sistema (uničenje ali poškodbe strojne opreme, okužbe z zlonamerno programsko opremo, vdori v računalniški informacijski sistem),
- kraja programske ali strojne opreme,
- izpad delovanja informacijskega sistema (strojna oprema, programska oprema, komunikacije),
- kršenje zakonodaje,
- neupoštevanje postopkov varovanja informacij.

17.4. PRIJAVA IN BELEŽENJE INCIDENTOV

Vsi zaposleni in pogodbeni sodelavci so dolžni prijavljati zaznane incidente Skrbniku SUVI. Prijava incidentov lahko poteka ustno, telefonsko, preko elektronske pošte ali preko prijavnega obrazca Registracija varnostnega incidenta.

Za celoten postopek poročanja o incidentih (zaznava, analiza in priglasitev skupinam CSIRT) je izključno odgovoren CISO oziroma Skrbnik SUVI. Postopek poteka samostojno in neposredno v skladu z zakonom.

17.5. UKREPANJE V PRIMERU POJAVA INCIDENTA

V primeru pojava incidenta je skupina za informacijsko varnost dolžna ustrezno ukrepati.

Glede na vrsto incidenta se ukrepi delijo na:

17.5.1. Ukrepanje v primeru izgube, uničenja ali zlorabe osebnih podatkov, občutljivih osebnih podatkov in zaupnih podatkov

V primeru incidentov, ki lahko povzročijo ali so povzročili izgubo, uničenje ali zlorabo osebnih podatkov, občutljivih osebnih podatkov ali zaupnih podatkov, je treba takoj izvesti ukrepe za zaščito teh podatkov in preprečitev nadaljnje škode. Postopek obravnave vključuje naslednje korake:

Prijava incidenta: Vsi zaposleni in pogodbeni sodelavci so dolžni zaznane incidente takoj prijaviti v Sektor za informatiko in skrbniku SUVI ustno, telefonsko, preko elektronske pošte ali preko obrazca *Registracija varnostnega incidenta*. V primeru neupravičenega dostopa ali suma neupravičenega dostopa do osebnih podatkov, mora prijava vsebovati natančen opis suma, vključno s specifičnimi podatki o osebi ali več osebah, ki naj bi v določenem obdobju, vendar omejeno na čas, ki ga določa veljavna zakonodaja na področju varstva osebnih podatkov, neupravičeno dostopale do osebnih podatkov.

Začasni zaščitni ukrepi: Takoj po prijavi incidenta se vzpostavijočasni zaščitni ukrepi, kar se izvede z vsemi strokovno usposobljenimi sodelavci (zaposleni, pogodbeni sodelavci), kot so omejitev dostopa do prizadetih informacijskih sistemov in zaščita preostalih podatkov.

Prva ocena incidenta: Skrbnik SUVI, opravi prvo oceno resnosti incidenta ter vključi skupino za informacijsko varnost v kolikor oceni, da je to potrebno ter pregleda sam ali s pomočjo skupine, revizijske sledi dostopov do izgubljenih, uničenih ali zlorabljenih podatkov ter ugotovi, kdo in kdaj je povzročil incident. **Vključitev drugih strokovnjakov:** Po potrebi se vključijo dodatni strokovnjaki s področja IT, pravne službe ali zunanji svetovalci za varnost podatkov. Če incident vključuje osebne podatke, se v postopek vključi pooblaščen oseba za varstvo osebnih podatkov (DPO), ki oceni vpliv na pravice posameznikov in poda priporočila za nadaljnje ukrepe.

Preverjanje sledljivosti: Za zagotovitev popolne sledljivosti in ugotovitev vzrokov za incident se poleg pregleda revizijskih sledi lahko izvedejo še dodatne aktivnosti, kot so intervjuji z vključenimi zaposlenimi ali pogodbenimi sodelavci, analiza dostopnih pravic in pregled sistemskih dnevnikov. S temi ukrepi se pridobi jasn vpogled v to, kdo je imel dostop do podatkov ter na kakšen način so se dostopne pravice uporabljale.

Izvajanje korektivnih ukrepov: Skrbnik SUVI, Skupina za informacijsko varnost ter po potrebi DPO, pripravijo načrt korektivnih ukrepov, ki lahko vključuje:

- uvedbo dodatnih varnostnih nastavitvev za preprečevanje podobnih incidentov,
- obvestilo prizadetim posameznikom, če je potrebno, in prijavo incidenta pristojnim organom.

Sankcije in nadzor: Po ugotovitvi odgovornosti se uvedejo ustrezne sankcije za zaposlene ali pogodbene sodelavce, ki so povzročili incident. Sankcije lahko vključujejo:

- Opozorilo ali pisni opomin: Prva stopnja sankcije za manjše kršitve, ki opozori posameznika na kršitev varnostnih postopkov.
- Izredna odpoved pogodbe o zaposlitvi: V primerih hujših kršitev ali namernih zlorab, ki ogrozijo varnost osebnih podatkov, lahko sledi izredna odpoved delovnega razmerja v kolikor je ta odpoved skladna z zakonodajo
- Ukinitve sodelovanja za pogodbene sodelavce: V primeru pogodbene kršitve s strani zunanjih sodelavcev se lahko prekine pogodba o sodelovanju ter se zahteva pokritje škode in nastalih posledic, ki so nastale kot posledica kršitev.

17.5.2. Ukrepanje v primeru poškodovanja, zlorabe ali izpada delovanja informacijskega sistema ter kraje programske in strojne opreme

V primeru incidentov, ki lahko povzročijo oziroma so povzročili namerno ali nenamerno poškodovanje ali zlorabo računalniškega informacijskega sistema, krajo opreme oziroma izpad delovanja računalniškega informacijskega sistema, je potrebno poskrbeti za primerno zaščito strojne in programske opreme (prenos sredstev na varno mesto, omejitev dostopa) oziroma ponovno vzpostavitev delovanja informacijskega sistema. Primarne aktivnosti so namenjene vzpostavitvi komunikacijskih povezav in delovanju opreme v območju računalniškega informacijskega sistema in komunikacijskega sistema in območju prostorov zdravstvene dejavnosti. Izvede se primerne varnostne ukrepe za ponovno vzpostavitev delovanja informacijskega sistema ter uvede sankcije za zaposlene ali pogodbene sodelavce, odgovorne za incident.

17.5.3. Ukrepanje v primeru kršenja zakonodaje

V primeru incidentov, ki predstavljajo direktno kršitev zakonodaje s področja varovanja podatkov, OI obvesti ustrezne državne organe. Izvede se primerne varnostne ukrepe za zmanjšanje škode ter uvede sankcije za zaposlene ali pogodbene sodelavce, odgovorne za incident.

17.5.4. Ukrepanje v primeru neupoštevanja postopkov varovanja informacij

V primeru incidentov, ki bi lahko bili posledica oziroma so posledica neupoštevanja postopkov varovanja informacij, je potrebno zagotoviti primerno zaščito informacij in informacijskega sistema ter zabeležiti vse značilnosti incidenta. Izvede se primerne varnostne ukrepe ter uvede sankcije za zaposlene ali pogodbene sodelavce, odgovorne za incident.

17.6. PREGLEDOVANJE IN OCENA INCIDENTOV

Po zaključenem reševanju incidenta skrbnik SUVI ter po potrebi in glede na naravo incidenta s pomočjo Skupine za informacijsko varnost ter drugih strokovnjakov oceni posledice incidenta in ukrepe, ki so bili izvedeni na podlagi incidenta. Oceni se vrsta incidenta, število prizadetih uporabnikov, količina in stopnja zaupnosti izgubljenih, uničenih ali zlorabljenih podatkov, čas trajanja in pogostost pojavljanja.

Strokovne evidence vodi CISO oziroma skrbnik SUVI, ki pripravi tudi letno poročilo za vodstvo.

Zaposleni in pogodbeni sodelavci so dolžni sodelovati s skrbnikom SUVI, skupino za informacijsko varnost ter ostalimi vključenimi strokovnjaki, da se incidenti lahko rešijo in da se podatki ustrezno zaščitijo. Po končanem ugotavljanju odgovornosti za incident Skrbnik SUVI z morebitno pomočjo skupine za informacijsko varnost, v kolikor jo je v to vključil, pripravi poročilo, ki ga posreduje direktorju OI. Na podlagi ugotovitev poročila se lahko sprejme primerne ukrepe, ki izboljšajo postopke varovanja informacij, ter predlaga uvedbo delovnopравnih postopkov za zaposlene ali sankcij za pogodbene sodelavce, odgovorne za incident.

POLITIKA UPORABE ZASEBNIH NAPRAV (BYOD) V DELOVNEM OKOLJU

Namen: Opis pravil v primeru uporabe zasebnih naprav v delovnem okolju

18.1. TERMINOLOŠKI SLOVAR

Zasebna IKT naprava: Informacijsko-komunikacijska naprava v lastni posameznika.

BYOD: Bring Your Own Device – koncept oziroma politika uporabe zasebnih IKT naprav (računalnikov, tablic, telefonov) v službenem okolju.

18.2. NAMEN POLITIKE UPORABE ZASEBNIH NAPRAV (BYOD) V DELOVNEM OKOLJU

Z dopuščanjem uporabe zasebnih naprav v službene namene se odpirajo resna varnostna vprašanja. Te naprave so kupili zaposleni sami, jih sami vzdržujejo in niso vezani na varnostne politike OI. Možnosti za nadzor take naprave so omejene.

Namen politike je opredeliti postopke in ukrepe s katerimi zagotovimo varno uporabo zasebnih naprav v delovnem okolju.

18.3. ZAHTEVE ZA UPORABO ZASEBNIH NAPRAV V DELOVNEM OKOLJU

Vsaka naprava mora zadoščati naslednjim zahtevam:

- Dostop do naprave mora biti varen (PIN, prstni odtis, geslo)
- Šifrirana komunikacija (VPN dostop – odobrene pravice s strani OI), ki je omejena na RDP protokol
- Za prenosne računalnike je obvezna uporaba antivirusnega programa

18.4. REGISTER ODOBRENIH VPN DOSTOPOV IN NJIHOVIH UPORABNIKOV

Sektor za informatiko vodi evidenco odobrenih VPN dostopov in njihovih uporabnikov. V primeru prenehanja delovnega razmerja pravice VPN dostopa prenehajo za vse morebitne zasebne naprave z ukinitvijo domenskega dostopa.

18.5. PRIJAVA IN BELEŽENJE INCIDENTOV

Vsi zaposleni so dolžni prijavljati zaznane incidente Skupini za obravnavo varnostnih incidentov. V primeru zaznanega incidenta, Skupina za obravnavo varnostnih incidentov sproži postopke skladno s Politiko upravljanja varnostnih incidentov.

SKLADNOST IN MERLJIVOST

Namen: Zagotavljanje skladnosti z regulatornimi zahtevami in merljivosti doseganja ciljev

19.1. NAMEN POLITIKE SKLADNOSTI IN MERLJIVOSTI

Namen politike je zagotavljanje skladnosti z regulatornimi zahtevami in merljivosti doseganja ciljev.

19.2. MERLJIVOST

Z namenom zagotavljanja preglednosti delovanja in skladnosti informacijske podpore z veljavnimi predpisi ter medicinskimi in poslovnimi potrebami z namenom spodbujanja doseganja ciljev se zagotavlja stalno merljivost in spremljanje.

OI ima zato glede informacijske podpore vzpostavljene naslednje notranje kontrole:

- večstopenjsko preverjanje in potrjevanje dobave in prevzema ter zaračunavanja prevzema storitev in blaga,
- redno poročanje organom OI (vodstvo, strokovni svet, svet zavoda, ...),
- redno poročanje o skladnosti z veljavnimi predpisi, pravili ZZS in metodološkimi navodili NIJZ.

19.3. SKLADNOST

Za zagotavljanje skladnosti informacijske podpore se upošteva notranje in zunanje vplive na OI, vključno z zahtevami:

- veljavnih predpisov EU in RS,
- mednarodnih in evropskih standardov, priporočil in smernic,
- pogodbenih obveznosti OI,
- internih aktov OI.

Vodstvo OI odločno podpira pokazati zavezanost k učinkovitosti informacijske podpore in varnosti informacij z določitvijo tega sistema politik upravljanja varnosti informacij, zagotavljanjem potrebnih virov, vzpostavitvijo vlog in odgovornosti ter spodbujanjem kulture varnosti informacij znotraj organizacije.

Seznam zahtev je sistematično vključen v vse procese razvoja in izvajanja informacijske podpore ter SUVI. To zagotavlja, da so vsi varnostni ukrepi in kontrolni mehanizmi oblikovani tako, da neposredno prispevajo k skladnosti z regulatornimi zahtevami.

Ustrezna dokumentacija in vodenje evidenc sta temelj za dokazovanje skladnosti z regulatornimi zahtevami. To vključuje politike, postopke, rezultate ocenjevanja tveganj, odločitve o nadzornih ukrepih ter zapisnike o vseh pomembnejših odločitvah ter usposabljanju in ozaveščanju zaposlenih.

Ker se zahteve lahko sčasoma spreminjajo ali ker pride do sprememb v organizaciji ali procesih OI ali zaradi tehnološkega razvoja, se redno pregleduje in posodablja seznam zahtev ter interni akti in SUVI. Enkrat letno se izvede pregled ažurnosti seznama vseh zahtev in skladnosti informacijske podpore.

19.4. ZAGOTAVLJANJE KAKOVOSTI

Varovanje informacij ob hkratnem zagotavljanju kakovosti je ključno za zagotavljanje visoke ravni in zakonitosti poslovanja ter zagotavljanje družbene odgovornosti OI. Zato je usmeritev v varovanje informacij skladna in tesno povezana z usmeritvijo v sisteme upravljanja kakovosti, varstva okolja, korporativne odgovornosti ali sorodne sisteme v skladu z mednarodnimi standardi.

OI ima vzpostavljen in vzdržuje sistem upravljanja kakovosti, ki zagotavlja standarden, formaliziran in kontinuiran pristop k varovanju informacij ob hkratnem zagotavljanju kakovosti. Vzpostavljeni sistem omogoča skladno delovanje tehnologije in poslovnih procesov s poslovnimi zahtevami. V OI se osredotoča na kakovostno upravljanje strank z identifikacijo njihovih zahtev, pri čemer se določa,

načrtuje in izvaja meritve za spremljanje zadovoljstva strank s kakovostjo. Pridobljene informacije se uporabijo za izboljšanje kakovosti. Sistem upravljanja kakovosti spodbuja kontinuirano izboljševanje.

19.5. UPRAVLJANJE PODATKOVNIH VIROV

V OI je vzpostavljena strategija glede upravljanja podatkovnih virov organizacije, s katero so seznanjeni vsi deležniki. Ključna so predvsem sledeča načela:

- dodelitev vlog in odgovornosti, kjer se zagotovi, da so korporativni podatki upravljani kot ključni viri in da se strategija upravljanja podatkov izvaja in vzdržuje na učinkovit in trajnosten način;
- vzpostavitev procesov in infrastrukture za določanje in razširjanje metapodatkov o podatkovnih virih organizacije, ki spodbujajo in podpirajo deljenje podatkov, zagotavljajo skladno rabo podatkov, izboljšujejo odzivnost na poslovne spremembe in zmanjšujejo tveganje povezano s podatki;
- opredelitev strategije za doseganje in vzdrževanje ravni kakovosti podatkov (kot so kompleksnost, integriteta, natančnost, popolnost, veljavnost, sledljivost in pravočasnost), potrebne za podporo poslovnim ciljem in nalogam;
- uvedba standardizirane metodologije, procesov, prakse, orodij in predlogov za profiliranje podatkov, ki se lahko uporabljajo v več podatkovnih repozitorijih in skladiščih podatkov skladno s predpisi, ki urejajo področje varstva podatkov;
- vzpostavitev sistematičnega pristopa za merjenje in vrednotenje kakovosti podatkov, glede na procese in tehnike ter v skladu s pravili zagotavljanja kakovosti podatkov;
- opredelitev mehanizmov, pravil, procesov in metod za preverjanje in popraviljanje podatkov v skladu s predhodno določenimi strateškimi cilji in poslovnimi usmeritvami;
- skrb, da organizacija spremlja, popisuje in nadzoruje tok podatkov skozi poslovne procese v življenjskem ciklu podatkov;
- zagotavljanje, da vzdrževanje podatkov izpolnjuje organizacijske in zakonske zahteve glede razpoložljivosti podatkov;
- zagotavljanje, da so izpolnjene zahteve veljavnih predpisov glede arhiviranja in hrambe podatkov.