ONKOLOŠKI INŠTITUT LJUBLJANA

Naziv dokumenta:	**KROVNA POLITIKA VAROVANJA INFORMACIJ**
Namen dokumenta:	Dokument opisuje pravila varovanja informacij Onkološkega inštituta Ljubljana
Številka dokumenta:	**2.0**
Verzija:	**2.0**
	Število strani: **33**

Referenčni dokument:	**Zakon o varstvu osebnih podatkov (ZVOP-1)** **Zakon o zdravstveni dejavnosti (ZZDej)** **Pravilnik o varstvu osebnih in drugih podatkov na Onkološkem inštitutu Ljubljana z dne 3.7.2019**

Dokument je namenjen seznanitvi zaposlenih ter določenih pogodbenih sodelavcev in vsebuje informacije, ki so namenjene samo osebam, ki jih potrebujejo pri izvajanju svojega dela.

Pregledal (skrbnik):	**Odobrila:**
Igor Josipović	v.d. generalne direktorice
Skrbnik SUVI	Andreja Uštar

REPUBLIKA SLOVENIJA ONKOLOŠKI INŠTITUT LJUBLJANA 3

Dne: 17 -12- 2020

Onkološki inštitut Ljubljana, Zaloška cesta 2, 1000 Ljubljana

E-pošta: info@onko-i.si
www.onko-i.si

KAZALO:

Politika klasifikacije informacij	**3**
Politika fizične zaščite in fizičnega dostopa	**5**
Politika dostopa do informacij, aplikacij in informacijskih sistemov	**8**
Politika dostopa do omrežja	**10**
Politika razvoja, spreminjanja in vzdrževanja aplikacij	**12**
Politika sprememb informacijskega sistema	**14**
Politika revizijskih sledi	**15**
Politika uporabe storitev interneta	**17**
Politika upravljanja in varovanja gesel	**19**
Politika varovanja v povezavi z zaposlenimi	**21**
Politika upravljanja kakovosti in varnosti storitev pogodbenih sodelavcev	**23**
Politika zaščite delovanja informacijskega sistema	**25**
Politika zaščite pred zlonamerno programsko opremo	**27**
Politika izdelave in shranjevanja varnostnih kopij	**28**
Politika izdelave in shranjevanja arhivskih dokumentov	**30**
Politika upravljanja z varnostnimi incidenti	**31**
Politika uporabe zasebnih naprav (BYOD) v delovnem okolju	**33**

POLITIKA KLASIFIKACIJE INFORMACIJ	
Namen:	Opis pravil klasificiranja podatkov Onkološkega inštituta Ljubljana

1. Terminološki slovar

Klasifikacija informacij – razvrstitev podatkov glede na varnostne zahteve.

2. Namen politike klasifikacije informacij

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

3. Lastništvo informacij

Onkološki inštitut Ljubljana (nadalje: OI) je lastnik informacij, ki je nahajajo na medijih OI in 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:

3.1. Osebni podatki

Osebni podatki se uporabljajo v poslovnih procesih OI in se nanašajo na posameznika (zaposlenega, pogodbenega sodelavca, uporabnika storitev). Osebne podatke lahko obdelujejo le zaposleni Onkološkega inštituta Ljubljana zaradi izvajanja delovnih obveznosti. Osebne podatke se varuje v območjih prostorov zdravstvene dejavnosti, upravne dejavnosti in računalniškega informacijskega sistema ter komunikacijskega sistema. Njihovo nepooblaščeno razkritje lahko resno škodi OI.

3.2. Občutljivi osebni podatki

Občutljivi osebni podatki se uporabljajo v poslovnih procesih OI in predstavljajo osebne podatke v zvezi z zdravjem oz. vsi podatki o zdravstvenem stanju posameznika. Občutljive osebne podatke lahko obdelujejo le zaposleni OI zaradi izvajanja delovnih obveznosti. Občutljive osebne podatke se varuje v varovanih območjih (predalniki, omare, blagajne) prostorov zdravstvene dejavnosti, upravne dejavnosti in računalniškega informacijskega sistema ter komunikacijskega sistema. Njihovo nepooblaščeno razkritje lahko zelo resno škodi OI.

3.3. Poslovna skrivnost

Poslovno skrivnost se uporablja v poslovnih procesih OI. Takšni podatki so interni postopki in navodila, statistike itd. v kolikor niso informacije javnega značaja. Klasifikacijo določijo pooblaščene osebe skladno s Pravilnikom o varstvu osebnih in drugih podatkov na Onkološkem inštitutu Ljubljana. Njihovo nepooblaščeno razkritje lahko škodljivo vpliva na poslovanje OI.

3.4. Javno

Vsi podatki, za katere pooblaščene 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.

4. Lastništvo in dovoljenje do dostopa

Do posameznih sklopov podatkov lahko dostopajo osebe, v skladu s svojimi delovnimi nalogami in pooblastili..

5. 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.

6. Označevanje informacij

Osebni podatki, občutljivi osebni podatki ter poslovna skrivnost, morajo biti od nastanka do uničenja obvladovani na način, da je zagotovljena sledljivost uporabe podatkov.
V primeru zahteve po javni objavi podatkov, ki so določeni kot poslovna skrivnost, generalni direktor in strokovne službe presodijo ali je podatke potrebno posredovati v javnost.

7. Nadzor

Skrbnik SUVI je v primeru zaznanih incidentov skupaj z pogodbenim sodelavcem dolžan preverjati upoštevanje pravilne klasifikacije informacij. V primeru zaznanega neustreznega ravnanja mora biti obveščen generalni direktor OI, ki sproži postopke skladno s Politiko upravljanja varnostnih incidentov ter Pravilnikom o varstvu osebnih in drugih podatkov na OI.

POLITIKA FIZIČNE ZAŠČITE IN FIZIČNEGA DOSTOPA	
Namen:	Opis pravil dostopanja do območij Onkološkega inštituta Ljubljana

1. Terminološki slovar

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

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

Strežniške in komunikacijske omare ter centralni podatkovni center: 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.

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. 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.

3.1. Območje javnega dostopa (prostori OI, kamor lahko dostopajo obiskovalci oziroma pogodbeni sodelavci)

Območje javnega dostopa ni posebej varovano, zato se v tem področju ne sme hraniti in obdelovati osebnih podatkov ali občutljivih osebnih podatkov ter poslovne skrivnosti. Obiskovalci ali pogodbeni sodelavci se v teh prostorih lahko nahajajo v skladu s hišnim redom OI. Območje javnega dostopa je fizično in tehnično varovano z varnostno službo ter videonadzorom.

3.2. Območje prostorov zdravstvene dejavnosti (prostori ambulant, bolnišničnih sob, prostorov za zdravstveno osebje, laboratorijev, kamor lahko dostopajo zaposleni OI oziroma pogodbeni sodelavci)

Območje prostorov zdravstvene dejavnosti je namenjeno hrambi in obdelavi osebnih podatkov ali občutljivih osebnih podatkov ter poslovne skrivnosti. OI zagotavlja primerno varovanje prostorov s prisotnostjo zaposlenih oziroma omejevanjem dostopa za obiskovalce (onemogočen nepooblaščen prehod obiskovalcev iz območja javnega dostopa v prostore zdravstvene dejavnosti). Dostop pogodbenih sodelavcev je možen izključno ob nadzorstvu zaposlenih, razen če odgovorna oseba določi drugače. Dostop do prostorov zdravstvene dejavnosti je urejen s kontrolo dostopa (ključ, brezkontaktna kartica). Prostori zdravstvene dejavnosti so izven delovnega časa zaklenjeni ter fizično in tehnično varovani z varnostno službo

3.3. Območje prostorov upravne dejavnosti

Območje prostorov upravne dejavnosti je namenjeno hrambi in obdelavi osebnih podatkov ali občutljivih osebnih podatkov ter poslovne skrivnosti. OI zagotavlja primerno varovanje prostorov s prisotnostjo zaposlenih oziroma omejevanjem dostopa za obiskovalce (zaklepanje pisarn, ko ni prisotnih zaposlenih). Dostop pogodbenih sodelavcev je možen izključno ob nadzorstvu zaposlenih, razen če odgovorna oseba določi drugače. Dostop do prostorov upravne dejavnosti je urejen s kontrolo dostopa (ključ, brezkontaktne kartice). Prostori upravne dejavnosti so izven delovnega časa zaklenjeni ter fizično in tehnično varovani z varnostno službo, določeni prostori tudi z alarmnim sistemom ter videonadzorom.

3.4. Območje računalniškega informacijskega sistema in komunikacijskega sistema (prostori s strežniško in komunikacijsko infrastrukturo)

Območje računalniškega informacijskega sistema in komunikacijskega sistema je namenjeno hrambi in obdelavi osebnih podatkov ali občutljivih osebnih podatkov ter poslovne skrivnosti. OI zagotavlja primerno varovanje prostorov z omejevanjem dostopa (ključi, brezkontaktne kartice) in evidentiranjem pristopa v območja.

Območje računalniškega informacijskega sistema in komunikacijskega sistema je zaklenjeno, razen v času izvajanja nalog zaposlenih Službe za informatiko in pogodbenih sodelavcev. Vsak dostop pogodbenih sodelavcev do območja se beleži (zapis v Evidenco prihodov in odhodov pogodbenih sodelavcev).

Komunikacijski kabli, po katerih se prenašajo informacije, so zaščiteni pred prestrezanjem ali poškodbami. Nameščajo se v ustrezne kanale. Vsi mrežni priključki, ki niso v uporabi, so neaktivni.

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 nepooblaščene 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).

5. Politika praznega zaslona

Zaposleni OI morajo zagotoviti, da nepooblaščenim osebam ni omogočen vpogled na računalniške zaslone. Vpogled lahko v posameznih primerih dovolijo zaposleni, če gre za obdelavo podatkov o uporabniku storitev, ki mora imeti vpogled v svoje osebne podatke ali občutljive osebne podatke.

Ob odhodu s svojega delovnega mesta morajo zaposleni OI zakleniti računalniško opremo (dostop omogočen izključno z uporabniškim imenom in geslom). V kolikor je odsotnost z delovnega mesta daljša od 30 minut, se računalniška oprema samodejno zaklene.

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 ali občutljivih osebnih podatkov ter poslovne skrivnosti.

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 zaposlenih med delovnim časom, fizično in tehnično varovanje izven delovnega časa). Za premeščanje računalniške opreme so zadolženi zaposleni Službe 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.

8. Nadzor nad fizičnim dostopom

Skrbnik SUVI vsaj 1x na mesec preverja, ali so bile za vse zaposlene in pogodbene sodelavce, ki so prenehali delovno razmerje ali pogodbeno sodelovanje, ukinjene pravice dostopa do posameznih območij OI.

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

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 pogodbene 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 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.

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.

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, ki je določen za vsakega posameznega zaposlenega OI ali pogodbenega sodelavca.

Pravice za dostop se zaposlenemu OI ali pogodbenemu sodelavcu določi glede na njegovo vlogo oziroma delovno mesto. Odobrene in dodeljene pravice omogočajo, da zaposleni OI ali pogodbeni sodelavec dostopa do tistih informacij, aplikacij in informacijskih sistemov, ki jih potrebuje za izvajanje svojega dela.

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

4. Dodelitev pravic dostopa

Ob prihodu novega zaposlenega ali pogodbenega sodelavca na Onkološki inštitut Ljubljana sproži postopek za dodelitev pravic dostopa kadrovska služba ob pomoči nadrejenega novozaposlenega. Novi zaposleni ali pogodbeni sodelavec 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 zaposleni ali pogodbeni sodelavec 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 dostopa se posreduje v Službo za informatiko, kjer so zadolženi za dodeljevanje 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

Zaposleni Službe za informatiko sporočijo uporabniška imena in gesla, ki jih novi zaposleni ali pogodbeni sodelavec potrebuje. Zaposleni Službe za informatiko so dolžni evidentirati vsako dodelitev pravic. Kadrovska služba skupaj s Skrbnikom SUVI vodi evidenco pravic dostopov do informacij, aplikacij in sistemov zaposlenih in pogodbenih sodelavcev.

5. Spremembe pravic dostopa

Zaposlenemu ali pogodbenemu sodelavcu se lahko v času njegove zaposlitve ali pogodbenega sodelovanja pravice do informacij, aplikacij in informacijskih sistemov lahko spremenijo. Vse zahteve morajo biti odobrene s strani vodje službe ali skrbnika pogodbenega sodelavca ter evidentirane pri Kadrovski službi.

6. Ukinitev pravic dostopa

Pravice dostopa se zaposlenemu ali pogodbenemu sodelavcu ukinejo v primeru zlorabe pravic, prekinitvi delovnega razmerja ali prenehanju pogodbenega sodelovanja.

V primeru zlorabe pravic zaposleni Kadrovske službe sporoči zaposlenim Službe za informatiko, ki urejajo pravice dostopa, da se takoj izvede ukinitev ali omejitev pravic dostopa.

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

Zaposleni Službe za informatiko po prejetem zahtevku za ukinitev pravic dostopa ukinejo vse pravice dostopa do informacij, aplikacij in informacijskih sistemov.

Nadzor nad pravicami dostopa do informacij, aplikacij in sistemov

Skrbnik SUVI redno preverja (najmanj enkrat mesečno) ali so bile za vse zaposlene in pogodbene sodelavce, ki so prenehali delovno razmerje ali pogodbeno sodelovanje, ukinjene pravice dostopa.

POLITIKA DOSTOPA DO OMREŽJA	
Namen:	Opis pravil dostopanja do omrežja OI

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.

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 zaposlenih OI in pogodbenih sodelavcev

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.

Zaposleni OI in pogodbeni sodelavci 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,
- neodobrene računalniške in mrežne opreme ni dovoljeno priklapljati v omrežje.

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).

4. Oddaljen dostop do omrežja OI

Oddaljen dostop do omrežja za zaposlene in pogodbene sodelavce se omogoči le tistim zaposlenim in pogodbenim sodelavcem, ki ga potrebujejo pri svojem delu. Dodelitev oddaljenega dostopa poteka v skladu s Politiko nadzora dostopa informacij, aplikacij in sistemov.

Do omrežja zaposleni in pogodbeni sodelavci z oddaljenih lokacij dostopajo preko VPN povezave, ki se zaključuje na požarni pregradi. Zaposleni in pogodbeni sodelavci se morajo za vzpostavitev VPN povezave overiti najmanj z uporabniškim imenom in geslom.

Zaposleni in pogodbeni sodelavci 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.

5. Nadzor dostopov do omrežja OI

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

Skrbnik SUVI je v primeru zaznanih incidentov dolžan preverjati 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

1. Terminološki slovar

Produkcijsko 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.

2. Namen politike za razvoj, spreminjanje in vzdrževanje aplikacij

Namen politike je opredeliti postopek razvoja, spreminjanja in vzdrževanja aplikacij, odgovornosti in naloge zaposlenih in pogodbenih sodelavcev OI, način nadzora ter dokumentacijo, ki jo je potrebno pri tem izdelati.

3. Izvajanje razvoja aplikacij

Razvoj aplikacij je projektno organiziran in se izvaja po predpisanih fazah:

3.1. Izbira pogodbenega sodelavca za razvoj aplikacije

Okvir za naročanje storitev pri pogodbenih izvajalcih postavlja veljavna zakonodaja na področju javnega naročanja. 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.

3.2. Razvoj aplikacije

Razvoj aplikacij poteka v razvojnem okolju pogodbenega sodelavca. Zaposleni Službe za informatiko in skrbnik pogodbenega sodelavca OI so odgovorni, da pogodbenega sodelavca že pred začetkom razvoja aplikacije seznanijo s postopki varovanja informacij, ki jih je dolžan upoštevati.

3.3. 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,
- navodilo za testiranje,
- uporabniški priročnik za zaposlene, ki bodo uporabljali aplikacijo.

3.4. 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 je funkcionalno oziroma po zmogljivostih enako produkcijskemu okolju.

Ko se z ustreznim postopkom testiranja ugotovi, da izdelana aplikacija zagotavlja v pogodbi opredeljeno funkcionalnost, zmogljivost in varnostne zahteve, zaposleni Službe za informatiko prenesejo aplikacijo v produkcijsko okolje.

3.5. Prevzem aplikacije

Za prevzem aplikacije je odgovoren vodja Službe za informatiko, ki odobri namestitev aplikacije v produkcijsko okolje informacijskega sistema OI.

3.6. Uvajanje zaposlenih za delo na aplikaciji

Pred ali po prenosu aplikacije v produkcijsko okolje se izvede usposabljanje zaposlenih za uporabo nove aplikacije ali sprememb nove verzije aplikacije.

4. Spreminjanje aplikacije

Spremembe aplikacije lahko predlaga vsak zaposleni, pri čemer navede razlog za spremembo in predlaga želeni rok izvedbe. Predlog odobri vodja Službe za informatiko. Zaposleni Službe za informatiko so odgovorni za pripravo specifikacij za spremembo aplikacij, ki se jih vključi v pogodbo s pogodbenim sodelavcem.

5. Vzdrževanje aplikacij

V kolikor zaposleni pri delu z aplikacijo naletijo na težave oziroma napake, jih sporočijo Skrbniku SUVI ali zaposlenim Službe za informatiko. Pri prijavi napake ali težave mora zaposleni 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 skrbnik SUVI in zaposleni Službe za informatiko, ki ugotovijo vzrok za težavo ali napako in po potrebi v reševanje vključijo razvijalca aplikacije. Če je vzrok za težavo ali napako take narave, da zahteva spremembo aplikacije, se sproži postopek za razvoj nove verzije aplikacije.

6. Nadzor

Skrbnik SUVI je v primeru zaznanih incidentov dolžan preverjati upoštevanje določil politike razvoja, spreminjanja in vzdrževanja aplikacij. V primeru zaznanega neustreznega ravnanja sproži postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA SPREMEMB INFORMACIJSKEGA SISTEMA	
Namen:	Opis pravil za upravljanje informacijskega sistema

1. Terminološki slovar

Produkcijsko 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, ki preverjajo možnost zlorab informacijskega sistema.

Vodstveni pregled: pregled stanja informacijske varnosti s strani generalne direktorice OI.

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.

3. Nabava programske in strojne opreme

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

4. Namestitev programske in strojne opreme

Programsko opremo se pred namestitvijo v produkcijsko okolje ustrezno testira v testnem okolju. Vsa programska oprema ustreza zahtevam licenčnih predpisov.

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

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

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.

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. Rezultate varnostnega pregleda se dokumentira v zapisniku vodstvenega pregleda.

POLITIKA REVIZIJSKIH SLEDI	
Namen:	Opis pravil glede vodenja revizijskih sledi nad podatki

1. Terminološki slovar

Revizijska sled: zapis podatkov o dogodkih pri dostopu do informacij, dogodkih v delovanju programske opreme in informacijskih sistemih.

Podatki o dostopih (vpogledih): evidenca dostopov ali vpogledov zaposlenih ali pogodbenih sodelavcev do osebnih podatkov, občutljivih osebnih podatkov ali poslovne skrivnosti ter dostopov z administratorskimi računi.

2. Namen politike za zagotavljanje revizijskih sledi

Politika določa postopke zagotavljanja sledljivosti dostopov do informacij, aplikacij in informacijskih sistemov. Postopki omogočajo preverjanje dostopa zaposlenih in pogodbenih sodelavcev v primeru zlorabe oziroma nepooblaščenega dostopa, ki ima lahko za posledico razkritje osebnih podatkov, občutljivih osebnih podatkov ter poslovne skrivnosti OI.

3. 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 zaposlenih in pogodbenih sodelavcev.

Revizijske sledi se ščiti pred nepooblaščenim dostopom in spreminjanjem.

4. 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.

4.1. 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 zaposlenega ali pogodbenega sodelavca, 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.

4.2. Občutljivi osebni podatki

Drugi nivo sledljivosti velja za občutljive osebne podatke, kjer je omogočeno naknadno ugotavljanje, kdo je vnesel, spremenil ali izbrisal kakšen podatek, 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.

4.3. Sledljivost posredovanja osebnih podatkov, občutljivih osebnih podatkov in poslovne skrivnosti izven informacijskega sistema OI

Poleg sledljivosti v informacijskem sistemu OI, se vsako posredovanje osebnih podatkov, občutljivih osebnih podatkov ali poslovne skrivnosti (izven informacijskega sistema OI) zabeleži, da je mogoče

pozneje ugotoviti, kateri osebni podatki ali občutljivi osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi.

5. Sledljivost aktivnosti zaposlenih in pogodbenih sodelavcev z administrativnimi računi

Pogodbeni sodelavci zagotavljajo revizijsko sled nad dostopi do informacijskih sistemov zaposlenih in pogodbenih sodelavcev, ki imajo administratorske račune.

6. Dostop do hrambe podatkov o dostopih (vpogledih)

Podatki o dostopih (vpogledih) so v informacijskem sistemu OI in v evidenci dostopov do papirne dokumentacije. Seznanitev s podatki o dostopih (vpogledih) je omejena na skrbnika SUVI in s strani generalne direktorice pooblaščene osebe.

7. Nadzor

V primeru zaznanih incidentov Skrbnik SUVI dostopa do zbirke podatkov o vpogledih v osebne podatke, občutljive osebne podatke in poslovno skrivnost ter zbirke podatkov o aktivnostih zaposlenih in pogodbenih sodelavcev z administrativnimi računi. V primeru zaznanega neustreznega ravnanja sproži postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA UPORABE STORITEV INTERNETA	
Namen:	Opis pravil za dostop do elektronske pošte in svetovnega spleta

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.

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, nepooblaščene spremembe in izgube podatkov, možnost okužbe z zlonamerno programsko opremo in prepreči izpad storitev interneta.

3. Uporaba storitev interneta

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

4. Uporaba svetovnega spleta (www)

Zaposleni lahko dostopajo do svetovnega spleta preko ponudnika internetnih storitev OI.

Zaposlenim 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.

5. Omejevanje dostopa do svetovnega spleta

Dostopanje do določenih naslovov ali določenih vsebin se omeji. Vodja Službe za informatiko določa naslove ali vsebine, do katerih se bo tehnično omejil dostop.

6. Politika uporabe elektronske pošte

Elektronska pošta OI je namenjena službeni uporabi.

OI večini delavcev v službene namene, zagotovi elektronski naslov. Tem delavcem je uporaba le tega elektronskega naslova naložena. Delavci ne smejo omogočiti uporabe poštnega 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.

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

Zaposleni 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 zaposleni pri pošiljatelju ali službi za informatiko preveriti izvor elektronske pošte.

Zaposleni ne smejo uporabljati sistema elektronske pošte za:

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

Zaposleni mora prijaviti varnosti incident v skladu s Politiko upravljanja varnostnih incidentov v primeru, ko:

- protivirusna programska oprema odkrije škodljivo kodo,
- zaposleni sumi, da je elektronska pošta okužena z virusom.

Ko zaposleni prekine delovno razmerje, se dostop do njegove elektronske pošte ukine. Vsebina poštnega predala se po potrebi arhivira, zaposlenemu pa se omogoči, da pred tem morebitno zasebno pošto odstrani ali shrani na drug podatkovni medij. Na zahtevo zaposlenega se za obdobje 1 meseca lahko tudi aktivira odzivnik o ukinitvi elektronskega naslova..

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

7. Omejevanje uporabe elektronske pošte

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

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

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 v skladu s Politiko upravljanja varnostnih incidentov, skrbnik SUVI opravi nadzor.

POLITIKA UPRAVLJANJA IN VAROVANJA GESEL	
Namen:	Opis zahtev upravljanja z gesli za dostop do informacij, aplikacij in informacijskih sistemov

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 zaposlenih OI.

Gesla administratorskega računa: gesla skrbnika aplikacije ali informacijskega sistema.

2. Namen politike upravljanja in varovanja gesel

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

3. Varno ravnanje z gesli

Uporabniško ime in geslo je namenjeno posameznemu zaposlenemu ali pogodbenemu sodelavcu.

Po prejemu uporabniškega imena in gesla s strani Službe za informatiko je zaposleni ali pogodbeni sodelavec dolžan varovati svoje geslo in ga ne sme razkrivati drugim osebam.

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

Če zaposleni ali pogodbeni sodelavec zasledi malomarno ali zlonamerno ravnanje z gesli, mora to takoj sporočiti Službi za informatiko ali Skrbniku SUVI. Geslo mora zaposleni ali pogodbeni sodelavec spremeniti takoj, če obstaja sum na razkritje gesla, in o tem obvestiti Službo 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. Postopke za njih določa Skrbnik SUVI.

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

4. Redna menjava in izbira kakovostnega gesla

Pri izbiri in menjavi gesel so zaposleni in pogodbeni sodelavci dolžni upoštevati naslednja pravila:

- izbirati je potrebno gesla z najmanj 16 znaki,

Priporoča se, da:

- je geslo kompleksno;
- 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, tobodotrijeprostimeti).
- da geslo ne vsebuje angleških, nemških, španskih in ruskih besed;
- uporabo pogovornega jezika ali slenga

5. Dodatna pravila za izbiro gesel in hramba gesel za administratorske račune

Pri izbiri in menjavi gesel za administratorske račune so zaposleni Službe 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 Službe 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 Službe za informatiko v najkrajšem možnem času spremeniti.

6. Izbira in menjava gesel kontrole fizičnega dostopa (alarmni sistem)

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

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

7. 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.
Uporabniško ime: ime, ki se določi zaposlenemu ali pogodbenemu sodelavcu za dostop do informacij, aplikacij in informacijskih sistemov.

POLITIKA VAROVANJA V POVEZAVI Z ZAPOSLENIMI	
Namen:	Opis pravil v SUVI za zaposlene OI

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.

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.

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.

4. Varovanje informacij na Onkološkem inštitutu Ljubljana

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

4.1. Postopki pred zaposlitvijo

Pred zaposlitvijo Kadrovska služba OI in Skrbnik SUVI novo zaposlenega seznanita 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.

4.2. Postopki med zaposlitvijo

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.

4.3. Postopki ob prekinitvi zaposlitve

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 logičnega dostopa do informacij in informacijskega sistema. Odgovornosti in obveznosti glede varovanja informacij, ki veljajo tudi po koncu zaposlitve, so vključene v pogodbe o zaposlitvi.

5. 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

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.

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.

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:

1. izgubo, uničenje ali zlorabo osebnih podatkov, občutljivih osebnih podatkov ter poslovne skrivnosti,
2. poškodovanje ali zlorabo informacijskega sistema,
3. krajo programske ali strojne opreme,
4. izpad delovanja informacijskega sistema (strojna oprema, programska oprema, komunikacije),
5. kršenje zakonodaje,
6. 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.

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.

5. Nadzor pogodbenih sodelavcev

Pogodbenim sodelavcem zaposleni Službe 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.

POLITIKA ZAŠČITE DELOVANJA INFORMACIJSKEGA SISTEMA	
Namen:	Opis zahtev podporne infrastrukture za delovanje informacijskega sistema

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, ki so priključena v električno omrežje.

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.

3. Infrastruktura

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

3.1. Informacijski sistem v območju prostorov zdravstvene dejavnosti

Informacijski sistem, ki je v območju prostorov zdravstvene dejavnosti, zagotavlja visoko stopnjo razpoložljivosti. Računalniške naprave so nameščene na delovnih mestih zdravstvenega osebja in v prostorih, kjer je možnost fizičnega poškodovanja manjša ter so dvignjene od tal. Računalniške naprave so nameščene tako, da je možnost fizičnega poškodovanja manjša (zaščita pred izlivom vode, požarom, nenamernim poškodovanjem) ter da ni možnosti pregrevanja naprav. Komunikacijski in električni kabli so do računalniških naprav speljani po kabelskih kanalih.

3.2. Informacijski sistem v območju prostorov upravne dejavnosti

Informacijski sistem, ki je v območju prostorov upravne dejavnosti, zagotavlja srednjo stopnjo razpoložljivosti. Računalniške naprave so nameščene na pisarniških mizah v območju, kjer je možnost fizičnega poškodovanja manjša ter so dvignjene od tal. Komunikacijski in električni kabli so do računalniških naprav speljani po kabelskih kanalih.

3.3. Informacijski sistem v območju računalniškega informacijskega sistema in komunikacijskega sistema (strežniške in komunikacijske omare, centralni podatkovni center)

Informacijski sistem, ki je v območju računalniškega informacijskega sistema in komunikacijskega sistema, zagotavlja visoko stopnjo razpoložljivosti. Naprave so povezane v sistem brezprekinitvenega napajanja, ki zagotavlja nemoteno delo ob prekinitvi dobave električnega toka iz distribucijskega omrežja. V območju so okoljski parametri (temperatura, vlaga) v skladu s specifikacijami proizvajalca strojne opreme. Računalniške naprave so zaščitene pred udari električnega toka (prenapetostna zaščita) in so nameščene tako, da je možnost fizičnega poškodovanja manjša (zaščita pred izlivom vode, požarom, nenamernim poškodovanjem) ter da ni možnosti pregrevanja naprav. Računalniška oprema je zavarovana s primernim sistemom za obveščanje o kritičnih dogodkih (protipožarni alarmni sistem). Komunikacijski in električni kabli so do računalniških naprav speljani po kabelskih kanalih.

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 se izvaja najmanj 1-krat letno. Skrbnik SUVI je v primeru zaznanih incidentov dolžan 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

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.

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.

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.

Skrbnik SUVI v primeru zaznanih incidentov skupaj s pogodbenimi sodelavci preverja prisotnost zlonamerne programske opreme v informacijskem sistemu OI. V primeru zaznane zlonamerne programske opreme, skrbnik SUVI ali pogodbeni sodelavci sprožijo postopke skladno s Politiko upravljanja varnostnih incidentov.

POLITIKA IZDELAVE IN SHRANJEVANJA VARNOSTNIH KOPIJ	
Namen:	Opis pravil za varnostno kopiranje podatkov

1. Terminološki slovar

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

Ponovna vzpostavitev informacijskega sistema: postavitev 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.

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.

3. Izdelava varnostnih kopij podatkov na strežnikih

Pogostost izdelave varnostnih kopij ustreza varnostnim zahtevam poslovnih procesov OI, kar pomeni varnostno kopiranje vsak dan in prenos na oddaljeno lokacijo 1x na mesec. Za varnostno kopiranje se uporablja tračno enoto na lokaciji OI in 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.

Vsako varnostno kopiranje podatkov na tračno enoto se evidentira, pri čemer se zabeleži:

- čas izdelave varnostne kopije,
- uspešnost izdelave varnostne kopije,
- evidenčno številko varnostne kopije.

4. Shranjevanje varnostnih kopij

Varnostne kopije se hranijo v tračni enoti v območju računalniškega informacijskega sistema, kamor lahko dostopajo samo zaposleni Službe za informatiko in pogodbeni sodelavci.

Varnostne kopije podatkov se mesečno hranijo na oddaljeni lokaciji, do podatkov lahko dostopajo samo zaposleni Službe za informatiko.

5. Preverjanje varnostnih kopij

Skrbnik SUVI 1x letno preveri, da se podatki dejansko nahajajo na tračni enoti in da podatki niso poškodovani ali uničeni ter testira, ali bi bilo v primeru dogodka ali varnostnega incidenta podatke mogoče restavrirati iz varnostnih kopij.

6. Nadzor izvajanja in shranjevanja varnostnih kopij

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

POLITIKA IZDELAVE IN SHRANJEVANJA ARHIVSKIH DOKUMENTOV	
Namen:	Opis pravil za hrambo podatkov

1. Terminološki slovar

Hramba: hramba podatkov za namene kasnejše rabe.

2. Namen politike za izdelavo in shranjevanje arhivskih dokumentov

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

3. Izdelava in hramba arhivskih dokumentov

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

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

4. Izdelava in hramba arhivskih dokumentov v papirni obliki

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

5. Izdelava in hramba arhivskih 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 arhivskih dokumentov se hrani v območju računalniškega informacijskega sistema in komunikacijskega sistema OI.

POLITIKA UPRAVLJANJA Z VARNOSTNIMI INCIDENTI	
Namen:	Opis postopkov v primeru pojava incidenta

1. Terminološki slovar

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

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. Incidente je potrebno skladno z 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.

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:

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

4. Prijava in beleženje incidentov

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

Skrbnik SUVI je dolžan beležiti vse podatke o prijavljenih incidentih, vodi evidenco incidentov in pripravlja in izvaja aktivnosti odprave oziroma zmanjšanja posledic incidentov.

5. Ukrepanje v primeru pojava incidenta

V primeru pojava incidenta je skrbnik SUVI dolžan ustrezno ukrepati. Glede na vrsto incidenta se ukrepi delijo na:

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

V primeru incidentov, ki lahko povzročijo oziroma so povzročili izgubo, uničenje ali zlorabo osebnih podatkov, občutljivih osebnih podatkov in zaupnih podatkov, je potrebno takoj poskrbeti za izvajanje ukrepov za zaščito podatkov. Preostale podatke se mora primerno zaščititi z ustreznimi varnostnimi ukrepi, kar se izvede z vsemi strokovno usposobljenimi sodelavci (zaposleni, pogodbeni sodelavci).

Revizijske sledi dostopov do izgubljenih, uničenih ali zlorabljenih podatkov se mora preveriti, da se ugotovi, kdo in kdaj je povzročil izgubo, uničenje ali zlorabo podatkov. Izvede se primerne varnostne ukrepe za zavarovanje informacijskega sistema ter uvede sankcije za zaposlene ali pogodbene sodelavce, odgovorne za incident ter izvede druge ukrepe v skladu z veljavno zakonodajo.

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.

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.

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.

6. Pregledovanje in ocena incidentov

Po zaključenem reševanju incidenta mora Skrbnik SUVI oceniti 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.

Skrbnik SUVI pripravi letno poročilo vseh zaznanih incidentov in ga preda generalni direktorici OI.

Zaposleni in pogodbeni sodelavci so dolžni sodelovati s Skrbnikom SUVI, da se incidenti lahko rešijo in da se podatki ustrezno zaščitijo. Po končanem ugotavljanju odgovornosti za incident Skrbnik SUVI pripravi poročilo, ki ga posreduje generalni direktorici OI. Na podlagi ugotovitev poročila se lahko sprejme primerne ukrepe, ki izboljšajo postopke varovanja informacij, ter predlaga uvedbo delovnopravnih 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

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.

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.

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
- Za prenosne računalnike je obvezna uporaba primernega antivirusnega programa

4. Register odobrenih zasebnih naprav in uporabnikov

Skrbnik SUVI vodi register zasebnih naprav in njihovih uporabnikov. V primeru prenehanja delovnega razmerja je potrebno takoj odvzeti pravice dostopa za vse morebitne zasebne naprave.

5. Prijava in beleženje incidentov

Vsi zaposleni so dolžni prijavljati zaznane incidente Skrbniku SUVI OI. V primeru zaznanega incidenta, skrbnik SUVI sproži postopke skladno s Politiko upravljanja varnostnih incidentov.