Univerzitetni rehabilitacijski inštitut
Republike Slovenije - Soča

Naziv dokumenta:	**KAZALO PODROČNIH POLITIK ZA POGODBENE PARTNERJE**
Namen dokumenta:	Dokument vsebuje naslednje področne politike namenjene pogodbenim partnerjem:

PO 04 Politika o navodilih za klasifikacijo

PO 08 Politika upravljanja in varovanja gesel

PO 09 Politika varovanja v zvezi z osebjem

PO 11 Politika upravljanja varnostnih incidentov

PO 14 Politika razvoja, spreminjanja in vzdrževanja programske opreme

PO 15 Politika nadzora sprememb informacijskega sistema

PO 16 Politika zaščite pred zlonamerno programsko opremo

PO 17 Politika upravljanja kakovosti in varnosti storitev tretjih strank

Dokument je namenjen seznanitvi pogodbenih partnerjev URI - Soča s Sistemom upravljanja informacijske varnosti - SUIV in vsebuje javno dostopne informacije.

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

Univerzitetni rehabilitacijski inštitut
Republike Slovenije - **Soča**

Naziv dokumenta:	**POLITIKA O NAVODILIH ZA KLASIFIKACIJO**	
Namen dokumenta:	Dokument opisuje razvrstitev podatkov glede na varnostne zahteve	
Številka dokumenta:	**PO 04 POLITIKA O NAVODILIH ZA KLASIFIKACIJO**	
Verzija:	**1**	
Stopnja zaupnosti:	**JAVNO**	**Število strani:** **4**
Datum odobritve:	**15.7.2015**	Dokument stopi v veljavo v 3 dneh od datuma odobritve.
Referenčni dokument:	**PO 03 Krovna politika varovanja informacij**	
Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.		
Pregledal (skrbnik): Vodja VIII, Glavna pisarna in arhiv Svetovalec VIII, Pravno področje	**Odobril:** Robert Prezelj, u.d.i.e., skrbnik SUIV	

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

TERMINOLOŠKI SLOVAR

- Klasifikacija podatkov – razvrstitev podatkov glede na varnostne zahteve

1 POLITIKA O NAVODILIH ZA KLASIFIKACIJO

1.1 Namen

Politika o navodilih za klasifikacijo, označevanje in ravnanje z informacijami določa pravila in postopke klasifikacije podatkov ter odgovornosti pri njihovem upravljanju. Pravila in postopki zmanjšajo možnost nepooblaščene uporabe, ki ima lahko za posledico razkritje podatkov izvajalca zdravstvene dejavnosti.

Pravila klasifikacije morajo biti usklajena z varnostnimi zahtevami in hkrati omogočati neovirano izvajanje zdravstvene dejavnosti. Določitev pravil temelji na razvrstitvi informacij, zakonodaji in pogodbenih obveznostih, ki zadevajo zaščito dostopov do informacij in storitev. Politiko o navodilih za klasifikacijo, označevanje in ravnanje z informacijami je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

1.2 Lastništvo in informacije

Posamezen izvajalec zdravstvene dejavnosti je lastnik vseh informacij, s katerimi v procesu upravlja. To so informacije, ki se uporabljajo za izvrševanje delovnih nalog. Lastniki informacij so odgovorni za določanje primerne stopnje klasifikacij informacij, ki so opredeljene kot:

1.2.1 Občutljivi osebni podatki

Občutljivi osebni podatki (Zakon o varstvu osebnih podatkov) se uporabljajo pri izvajalcu zdravstvene dejavnosti in predstavljajo opis zdravstvenega stanja posameznika ne glede na obliko, v kateri so izraženi. Njihovo nepooblaščeno razkritje lahko zelo resno škodi izvajalcem zdravstvene dejavnosti in njihovim uporabnikom.

1.2.2 Osebni podatki

Osebni podatki (Zakon o varstvu osebnih podatkov) se uporabljajo pri izvajalcu zdravstvene dejavnosti in se nanašajo na posameznika ne glede na obliko, v kateri so izraženi. Njihovo nepooblaščeno razkritje lahko resno škodi izvajalcem zdravstvene dejavnosti in njihovim uporabnikom.

1.2.3 Samo za interno rabo (poslovna skrivnost)

Vsi podatki, ki ne sodijo v zgornjo klasifikacijo, vendar je njihovo nepooblaščeno razkritje v nasprotju s politiko varovanja informacij. Podatki lahko ob razkritju škodljivo vplivajo na izvajalca zdravstvene dejavnosti in njegove uporabnike. Takšni primeri so določeni s sklepom o varovanju poslovne skrivnosti, ki ga izda generalni direktor inštituta.

1.2.4 Javno

Vsi podatki, za katere je izvajalec zdravstvene dejavnosti dovolil, da se jih sme javno objaviti. Za take informacije tudi nepooblaščeno razkritje ne pomeni grožnje. Primeri takšnih informacij so objave v medijih.

1.3 Lastništvo in dovoljenje do dostopa

Lastniki morajo odločati o tem, kdo pridobi dovoljenje dostopa do informacij in na kakšen način se bo s to informacijo ravnalo glede na njeno klasifikacijo. Lastniki določijo, kako se bo izvajal primeren nadzor pri hranjenju, ravnanju, širjenju in drugi uporabi informacij.

1.4 Odgovornosti uporabnikov informacij

Vsi uporabniki informacijskega sistema izvajalca zdravstvene dejavnosti, ki pridejo v stik z občutljivimi osebnimi podatki in osebnimi podatki ter podatki, ki so klasificirani samo za interno rabo ali javno, morajo poznati politiko o navodilih za klasifikacijo, označevanje in ravnanje z informacijami ter jo učinkovito izvajati kot del vsakodnevnih nalog pri delu.

1.5 Označevanje informacij

Občutljivi osebni podatki in osebni podatki ter podatki, ki so klasificirani samo za interno rabo so lahko od nastanka do uničenja označeni s primerno oznako klasifikacije informacij ali hranjeni tako, da je jasno razvidna klasifikacijska oznaka. Takšne oznake se morajo nahajati na vseh izvodih informacije, tako v elektronski kot fizični obliki. Uporabniki ne smejo odstranjevati ali spreminjati oznak klasifikacije informacij, razen če so za to prejeli dovoljenje lastnika.

1.6 Ravnanje z informacijami

Z vsemi informacijami je potrebno ravnati skrbno in skladno s krovno varnostno politiko in področnimi varnostnimi politikami glede na določila za posamezno klasifikacijsko oznako.

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča

Naziv dokumenta:	**POLITIKA UPRAVLJANJA IN VAROVANJA GESEL**		
Namen dokumenta:	Dokument opisuje pravila izbire, menjave in varovanja gesel		
Številka dokumenta:	**PO 08 POLITIKA UPRAVLJANJA IN VAROVANJA GESEL**		
Verzija:	**1**		
Stopnja zaupnosti:	**JAVNO**	**Število strani:**	**4**
Datum odobritve:	**15.7.2015**	Dokument stopi v veljavo v 3 dneh od datuma odobritve.	
Referenčni dokument:	**PO 03 Krovna politika varovanja informacij**		
Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.			
Pregledal (skrbnik): Inženir tehničnih strok VII/2 (I), Informacijska varnost		**Odobril:** Robert Prezelj, u.d.i.e., skrbnik SUIV	

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

TERMINOLOŠKI SLOVAR

- Administratorska gesla - uporabljajo skrbniki za dostop do sistemov in aplikacij in jim omogočajo izvajanje skrbniških opravil, ki vključujejo tudi dodeljevanje in ukinitev pravic dostopa uporabnikom do sistemov, podatkov in aplikacij
- Uporabniška gesla - uporabljajo uporabniki za prijavo v računalniško omrežje in za dostop do aplikacij in informacij
- Uporabnik - oseba, ki uporablja informacijski sistem
- Sistemski skrbnik - skrbnik posameznega informacijskega sistema

1 POLITIKA UPRAVLJANJA IN VAROVANJA GESEL

1.1 Namen

Namen dokumenta 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.

1.2 Varovanje gesel

Geslo uporabnika sistema je namenjeno samo njegovi uporabi, zato so uporabniki sistemov odgovorni za vse akcije, ki se zgodijo z uporabo njihove identitete.

Uporabniki s svojimi osebnimi gesli ravnajo kot s strogo zaupnimi informacijami in jih ne smejo razkrivati oziroma posojati drugim osebam. Če zaposleni zasledi malomarno ali zlonamerno ravnanje z gesli, to takoj sporoči nadrejenemu. Geslo mora uporabnik spremeniti takoj, če obstaja sum na razkritje gesla. O tem obvesti pooblaščeno osebo.

Uporabniki pri izbiri gesel upoštevajo osnovna varnostna pravila. Geslo ne sme vsebovati besed iz slovarja, imen in priimkov uporabnika in družinskih članov, katerekoli oblike datuma, imena, oznake ali številke organizacije, zaporednih števil.

Začasna gesla je zaposlenim potrebno pošiljati oziroma izročati na varen način.

Sistemski skrbnik, ki je odgovoren za dodelitev začasnega gesla, uporabniku ustno sporoči geslo, ki ga uporabnik spremeni ob prvi prijavi. Gesla zaposleni ne smejo zapisovati na papir ali shranjevati na kakršenkoli drug način, ki bi drugi osebi lahko omogočil dostop do gesla.

Če uporabnik geslo pozabi, mu sistemski skrbnik dodeli novo začasno geslo, ki ga uporabnik spremeni ob prvi prijavi.

1.3 Upravljanje in varovanje administratorskih gesel

Pri izbiri in menjavi gesel so skrbniki (zunanji izvajalci) dolžni upoštevati naslednja pravila:

- administratorska gesla imajo vsaj 10 znakov
- gesla vsebujejo najmanj 3 od naslednjih 4 tipov znakov: velike črke, male črke, števila, simboli
- gesla ne vsebujejo šumnikov
- gesla je potrebno menjati vsakih 90 dni
- vsaj 3 zaporedna gesla morajo biti neponovljiva

Vsa administratorska gesla sistemov in aplikacij je potrebno shraniti, da se v nujnih primerih zagotovi možnost dostopa do sistemov tudi v odsotnosti sistemskega skrbnika. Vsa administratorska gesla se hranijo v zaprtih kuvertah, ki so shranjene tako, da je onemogočen dostop nepooblaščenim osebam.

Na kuverto je potrebno napisati ime sistema oziroma aplikacije in datum, ko je bilo geslo zadnjič spremenjeno. Zaprto kuverto podpiše uporabnik gesla, ki je geslo shranil. V kuverti je zapisano, za katero administratorsko geslo gre ter uporabniško ime in geslo. Ob dodelitvi ali menjavi gesla sistemski skrbnik kuverto izroči pooblaščeni osebi, ki jo shrani tako, da je ustrezno zavarovana pred nepooblaščenimi dostopi.

Odprtje katerekoli kuverte z geslom v primeru nujnega posega se mora zabeležiti v evidenčni list. Zapisati je potrebno datum in čas odprtja kuverte z geslom, kdo je odprl kuverto in kdo je dostopal do gesla. Geslo mora sistemski skrbnik v najkrajšem možnem času spremeniti.

Redno menjavo gesla kontrolira oseba, odgovorna za delovanje informacijskega sistema, oziroma je zahtevana s strani informacijskega sistema.

1.4 Izbira in menjava uporabniških gesel

Pri izbiri in menjavi uporabniških gesel se priporoča upoštevati naslednja pravila:

- izbirati je potrebno gesla z najmanj 6 in največ 15 znaki
- geslo je sestavljeno iz najmanj 3 različnih znakov, od katerih je vsaj ena črka
- gesla ne vsebujejo šumnikov
- gesla je potrebno menjati vsakih 90 dni
- vsaj 3 zaporedna gesla so neponovljiva

Univerzitetni rehabilitacijski inštitut
Republike Slovenije - Soča

Naziv dokumenta:	**POLITIKA VAROVANJA V ZVEZI Z OSEBJEM**	
Namen dokumenta:	Dokument opisuje varnostne postopke, ki jih morajo upoštevati vsi zaposleni in uporabniki informacijskega sistema	
Številka dokumenta:	**PO 09 POLITIKA VAROVANJA V ZVEZI Z OSEBJEM**	
Verzija:	**1**	
Stopnja zaupnosti:	**JAVNO**	**Število strani: 4**
Datum odobritve:	**15.7.2015**	Dokument stopi v veljavo v 3 dneh od datuma odobritve.
Referenčni dokument:	**PO 03 Krovna politika varovanja informacij**	

Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.

Pregledal (skrbnik):	**Odobril:**
Varnostni inženir VII/2 (III), Inženir tehničnih strok VII/2 (I), Informacijska varnost Svetovalec VIII, Pravno področje	Robert Prezelj, u.d.i.e., skrbnik SUIV

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

TERMINOLOŠKI SLOVAR

- Pooblaščena oseba – oseba, ki ji vodstvo izvajalca zdravstvene dejavnosti podeli določene pravice
- Uporabniki informacijskega sistema – vsi, ki imajo dostop do informacij izvajalca zdravstvene dejavnosti
- Izjava o varovanju informacij – dokument, s katerim se oseba zaveže k varovanju informacij izvajalca zdravstvene dejavnosti

1 POLITIKA VAROVANJA V ZVEZI Z OSEBJEM

1.1 Namen

Izvajalec zdravstvene dejavnosti je odgovoren za pripravo in vzpostavitev varnostnih postopkov, ki jih morajo upoštevati in izvajati vsi zaposleni oziroma uporabniki informacijskega sistema in informacij. Z namenom čim boljšega poznavanja zahtev varnostnih postopkov mora izvajalec zdravstvene dejavnosti zagotavljati primerna izobraževanja in usposabljanja za zaposlene in uporabnike informacijskega sistema.

Dokument predstavlja okvir za upravljanje izvajanja varnostnih postopkov ter dolžnosti in pravic za zaposlene in uporabnike informacijskega sistema.

1.2 Varnostne politike

Vsi zaposleni in uporabniki informacijskega sistema so dolžni upoštevati vse dokumente sistema za upravljanje informacijske varnosti (v nadaljevanju: SUIV), ki je dostopen pri izvajalcu zdravstvene dejavnosti. Dokumenti SUIV opredeljujejo vsa področja dela izvajalcev zdravstvene dejavnosti in celovito obravnavajo varovanje podatkov ter določajo skladnost varovanja informacij z načinom dela izvajalca zdravstvene dejavnosti.

Za izvajanje primernih varnostnih ukrepov so zadolženi zaposleni in ostali uporabniki, ki dostopajo do informacij in informacijskega sistema izvajalca zdravstvene dejavnost. Vodstvo izvajalca zdravstvene dejavnosti je odgovorno za izvajanje mehanizmov varovanja informacij v celoti in za zagotovitev potrebnih virov, ki omogočajo primerno vodenje SUIV.

Vodstvo izvajalca zdravstvene dejavnosti je dolžno poskrbeti, da so dokumenti SUIV ustrezno objavljeni, tako da so varnostne politike na vpogled vsem zaposlenim in uporabnikom informacij in informacijskega sistema izvajalca zdravstvene dejavnosti

Vsako neupoštevanje pravil politik varovanja informacij in pripadajočih dokumentov SUIV šteje za kršitev pogodbe o delu ali pogodbe o sodelovanju in se kot tako tudi sankcionira.

1.3 Izobraževanje, usposabljanje in preverjanje

Vsi zaposleni in uporabniki informacijskega sistema morajo biti ustrezno izobraženi glede določil dokumentacije SUIV. Za izobraževanje je zadolžena pooblaščena oseba, ki jo določi vodstvo izvajalca zdravstvene dejavnosti.

Izobraževanje se mora opravljati ob prihodu novega zaposlenega ali uporabnika informacijskega sistema, stalno v času zaposlitve oziroma takrat, ko je to potrebno zaradi spremembe varnostne politike, postopkov ali navodil. Izobraževanja se morajo udeležiti vsi zaposleni.

Pooblaščena oseba lahko zahteva primerno poznavanje dokumentacije SUIV za zagotovitev primernega načina dela zaposlenih.

1.4 Varovanje informacij pri izvajalcih zdravstvene dejavnosti

Varovanje informacij se začne že pred samo zaposlitvijo ali uporabo informacijskega sistema in informacij, traja ves čas zaposlitve ali uporabe informacijskega sistema in se mora zagotavljati tudi po koncu zaposlitve ali uporabe informacijskega sistema izvajalca zdravstvene dejavnosti.

1.4.1 Pred zaposlitvijo ali uporabo informacijskega sistema

Pred zaposlitvijo ali uporabo informacijskega sistema in informacij mora pooblaščena oseba zagotoviti vpogled v dokumentacijo SUIV izvajalca zdravstvene dejavnosti ter bodočemu novo zaposlenemu ali uporabniku informacijskega sistema in informacij dati v podpis Izjavo o zaupnosti.

V pogodbi o zaposlitvi ali uporabi informacijskega sistema in informacij mora biti podan sklic na dokumentacijo SUIV in sankcije v primeru izgube, uničenja ali zlorabe informacij.

1.4.2 Med zaposlitvijo ali uporabo informacijskega sistema

Pooblaščena oseba lahko preverja, ali zaposleni upoštevajo vsa določila dokumentacije SUIV in v primeru neupoštevanja sprejema ustrezne ukrepe. Vse spremembe, ki vplivajo na delo ali varovanje informacij, morajo biti posredovane vsem zaposlenim in uporabnikom informacijskega sistema in informacij izvajalca zdravstvene dejavnosti.

Pripravljeni morajo biti postopki v primeru kršenja določil dokumentacije SUIV.

1.4.3 Po prekinitvi zaposlitve ali uporabe informacijskega sistema

Odgovornosti in obveznosti, ki veljajo tudi po prenehanju pogodbenega razmerja, morajo biti vključene v pogodbe z zaposlenimi ali uporabniki informacijskega sistema in informacij.

Vsi zaposleni ter uporabniki informacijskega sistema in informacij morajo ob koncu zaposlitve ali pogodbe vrniti vsa sredstva informacijskega sistema izvajalca zdravstvene dejavnosti, ki so jih prejeli v uporabo. Vsem zaposlenim ter uporabnikom informacijskega sistema in informacij je ob koncu zaposlitve potrebno odvzeti pravice fizičnega in logičnega dostopa do informacij in zmogljivosti za obdelavo informacij.

1.5 Odgovornost izvajalca zdravstvene dejavnosti

Izvajalec zdravstvene dejavnosti je odgovoren za vse kršitve varnostnih politik s strani zaposlenih ali uporabnikov informacijskega sistema in informacij, v kolikor nima vpeljanega, izvajanega in vzdrževanega SUIV.

Vsako neupoštevanje varnostnih politik s strani zaposlenih ali uporabnikov informacijskega sistema mora biti ustrezno obravnavano v skladu s Politiko upravljanja varnostnih incidentov.

Vodstvo izvajalca zdravstvene dejavnosti mora zagotavljati vsem zaposlenim primerna izobraževanja in dostop do dokumentacije SUIV. Vsako odstopanje od navedenega predstavlja neskladnost, za katero odgovarja izvajalec zdravstvene dejavnosti.

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča

Naziv dokumenta:	**POLITIKA UPRAVLJANJA VARNOSTNIH INCIDENTOV**	
Namen dokumenta:	Dokument opisuje postopke prijave, ukrepanja in analize varnostnih incidentov	
Številka dokumenta:	**PO 11 POLITIKA UPRAVLJANJA VARNOSTNIH INCIDENTOV**	
Verzija:	**1**	
Stopnja zaupnosti:	**JAVNO**	**Število strani: 5**
Datum odobritve:	**15.7.2015**	Dokument stopi v veljavo v 3 dneh od datuma odobritve.
Referenčni dokument:	**PO 03 Krovna politika varovanja informacij**	
Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.		
Pregledal (skrbnik): Inženir tehničnih strok VII/2 (I), Informacijska varnost	**Odobril:** Robert Prezelj, u.d.i.e., skrbnik SUIV	

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

TERMINOLOŠKI SLOVAR

- Pooblaščena oseba – oseba, ki ji vodstvo izvajalca zdravstvene dejavnosti podeli določene pravice
- Računalniški informacijski sistem – vse elektronske naprave in komunikacije, ki so namenjene obdelavi, prenosu in hrambi podatkov
- Tabela incidentov – mesto, kjer se nahajajo zapisi vseh zaznanih incidentov
- Prometni podatki – so kakršnikoli podatki, ki se obdelujejo zaradi prenosa komunikacij v elektronskem komunikacijskem omrežju
- Revizijske sledi – beleženje aktivnosti uporabnika v informacijskem sistemu
- Nadzorni mehanizmi – sredstva ali aktivnosti nadzorovanja uporabnikov informacijskega sistema

1 POLITIKA UPRAVLJANJA VARNOSTNIH INCIDENTOV

1.1 Namen

Izvajalec zdravstvene dejavnosti je odgovoren 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 pooblaščenim osebam. Incidente je potrebno skladno z varnostno politiko identificirati in reševati glede na kritičnost posameznega incidenta.

Dokument predstavlja okvir za upravljanje incidentov. Namen dokumenta je opredeliti postopke, s katerimi organizacija zagotovi, da se incidenti obvladujejo, oziroma da se odpravijo ali zmanjšajo posledice incidenta.

1.2 Definicija incidenta

Incident predstavlja en ali več nezaželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo lahko ogrozili normalno delovanje izvajalca zdravstvene dejavnosti oziroma zaupnost, celovitost ali razpoložljivost podatkov, do katerih izvajalec zdravstvene dejavnosti dostopa, jih obdeluje ali hrani.

Incidenti so:

- izguba, uničenje ali zloraba osebnih podatkov in občutljivih osebnih podatkov (podatki v elektronski obliki, papirni dokumenti itd.), ki vpliva na zaupnost, celovitost ali razpoložljivost podatkov;
- namerno ali nenamerno poškodovanje ali zloraba računalniškega informacijskega sistema (uničenje ali poškodbe strojne opreme, okužbe z zlonamerno programsko opremo, vdori v računalniški informacijski sistem), ki vpliva na razpoložljivost podatkov;
- kraja opreme (strojne ali programske);
- izpad delovanja računalniškega informacijskega sistema izvajalca zdravstvene dejavnosti (strojna oprema, programska oprema, komunikacije), ki vpliva na razpoložljivost podatkov in storitev;
- kršenje zakonodaje;
- neupoštevanje določil varnostnih politik s strani zaposlenih in tretjih strank.

1.3 Prijava in beleženje incidentov

Vsi zaposleni in uporabniki informacijskega sistema izvajalca zdravstvene dejavnosti so dolžni prijavljati zaznane incidente pooblaščeni osebi, ki jo določi izvajalec zdravstvene dejavnosti. Prijava incidentov lahko poteka ustno, telefonsko, preko elektronske pošte ali namenskih aplikacij. Pri prijavi incidenta je potrebno navesti:

- kaj se je zgodilo
- kje je bil zapažen incident
- kdaj je bil zapažen incident
- kdo je bil prisoten

- kakšne so posledice in kakšen vpliv ima incident na delovanje izvajalca zdravstvene dejavnosti oziroma zaupnost, celovitost ali razpoložljivost podatkov, do katerih izvajalec zdravstvene dejavnosti dostopa, jih obdeluje ali hrani.

Pooblaščena oseba je dolžna beležiti vse podatke o prijavljenih incidentih na enem mestu (tabela incidentov) in izvajati aktivnosti odprave oziroma zmanjšanja posledic incidentov.

Vsi incidenti, ki lahko povzročijo oziroma so povzročili izgubo, uničenje ali zlorabo osebnih podatkov ali občutljivih osebnih podatkov (podatki v elektronski obliki, papirni dokumenti itd.), morajo biti takoj sporočeni vodstvu javnega zdravstvenega zavoda.

Vsi incidenti, ki lahko povzročijo oziroma so povzročili namerno ali nenamerno poškodovanje ali zlorabo računalniškega informacijskega sistema, krajo strojne ali programske opreme oziroma izpad delovanja računalniškega informacijskega sistema izvajalca zdravstvene dejavnosti, ki vpliva na razpoložljivost podatkov, morajo biti v istem delovnem dnevu oziroma prvi delovni dan po incidentu sporočeni vodstvu javnega zdravstvenega zavoda.

Vsi incidenti, ki bi lahko bili posledica oziroma so posledica kršenja zakonodaje ali neupoštevanja določil varnostnih politik, morajo biti sporočeni v rednih poročilih vodstvu javnega zdravstvenega zavoda.

1.4 Ukrepanje v primeru pojava incidenta

V primeru pojava incidenta je pooblaščena oseba dolžna ustrezno ukrepati. Glede na vrsto incidenta se ukrepi delijo na:

1.4.1 Ukrepanje v primeru izgube, uničenja ali zlorabe podatkov

V primeru incidentov, ki lahko povzročijo oziroma so povzročili izgubo, uničenje ali zlorabo osebnih podatkov ali občutljivih osebnih podatkov (podatki v elektronski obliki, papirni dokumenti itd.), je potrebno takoj poskrbeti za izvajanje ukrepov za zaščito podatkov. Preostale podatke se mora primerno zaščititi z ustreznimi varnostnimi ukrepi, kar lahko pooblaščena oseba izvede z vsemi strokovno usposobljenimi sodelavci (informatiki, delavci splošnih služb, varnostniki itd.). 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. Na podlagi odgovora vodstva na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

1.4.2 Ukrepanje v primeru poškodovanja, zlorabe, izpada delovanja računalniškega sistema ali kraje 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 izvajalca zdravstvene dejavnosti, je potrebno poskrbeti za primerno zaščito računalniških informacijskih sredstev (prenos sredstev na varno mesto, omejitev dostopa) oziroma ponovno vzpostavitev delovanja računalniškega informacijskega sistema. Primarne aktivnosti so namenjene vzpostavitvi komunikacijskih povezav in delovanju opreme, namenjene za izvajanje zdravstvene dejavnosti. Na podlagi odgovora vodstva na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

1.4.3 Ukrepanje v primeru kršenja zakonodaje

V primeru incidentov, ki predstavljajo direktno kršitev zakonodaje, mora vodstvo takoj obvestiti ustrezne državne institucije (Policija) in v skladu z njihovimi navodili podati vse podatke oziroma predati sredstva, ki so bila uporabljena pri izvajanju prekrška oziroma kaznivega dejanja. Na podlagi odgovora vodstva na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

1.4.4 Ukrepanje v primeru neupoštevanja varnostnih politik

V primeru incidentov, ki bi lahko bili posledica oziroma so posledica neupoštevanje določil varnostnih politik, je potrebno zagotoviti primerno zaščito podatkov in računalniškega informacijskega sistema ter zabeležiti vse značilnosti incidenta. Na podlagi odgovora vodstva na poročilo o incidentu se izvede primerne varnostne ukrepe ter uvede sankcije za osebe, odgovorne za incident.

1.5 Pregledovanje in presojanje incidentov

Po zaključenem reševanju incidenta mora pooblaščena oseba 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.

Pooblaščena oseba o vseh incidentih najmanj enkrat letno obvešča vodstvo izvajalca zdravstvene dejavnosti.

Pooblaščena oseba ima odgovornost, da ugotavlja, kdo je bil udeležen v posameznem incidentu, v ta namen pa ima pravico do vpogleda v naslednje podatke:

- vsebina elektronske pošte (s privolitvijo osebe, ki ima ta elektronski naslov),
- prometni podatki elektronske pošte,
- prometni podatki dostopa do interneta,
- podatki, ki se nahajajo na računalniški opremi (lokalni disk, USB ključ, strežniška in omrežna infrastruktura itd.) – razen vsebine elektronske pošte in podatkov o dostopih do spletnih strani,
- revizijske sledi dostopa do osebnih podatkov in občutljivih osebnih (kdo in kdaj je podatek ustvaril, spremenil, izbrisal oziroma vpogledal vanj),
- podatki nadzornih mehanizmov (logi brezkontaktnih kartic, videonadzor, biometrija, vpisi v dnevnik dostopov itd.).

Zaposleni so dolžni sodelovati s pooblaščeno osebo, da se incidenti lahko rešijo in da se podatki ustrezno zaščitijo.

Po končanem ugotavljanju odgovornosti za incident pooblaščena oseba pripravi poročilo, ki se posreduje vodstvu izvajalca zdravstvene dejavnosti. Na podlagi ugotovitev poročila lahko vodstvo sprejme primerne ukrepe, ki lahko izboljšajo stanje varovanja informacij, ter uvede sankcije za osebe, odgovorne za incident.

Univerzitetni rehabilitacijski inštitut
Republike Slovenije - **Soča**

Naziv dokumenta:	**POLITIKA RAZVOJA, SPREMINJANJA IN VZDRŽEVANJA PROGRAMSKE OPREME**	
Namen dokumenta:	Dokument opisuje postopek razvoja in vzdrževanja programske opreme	
Številka dokumenta:	**PO 14 POLITIKA RAZVOJA, SPREMINJANJA IN VZDRŽEVANJA PROGRAMSKE OPREME**	
Verzija:	**1**	
Stopnja zaupnosti:	**JAVNO**	**Število strani:** **6**
Datum odobritve:	**15.7.2015**	Dokument stopi v veljavo v 3 dneh od datuma odobritve.
Referenčni dokument:	**PO 03 Krovna politika varovanja informacij**	
Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.		
Pregledal (skrbnik): Vodja I, Vodja službe za informatiko	**Odobril:** Robert Prezelj, u.d.i.e., skrbnik SUIV	

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

TERMINOLOŠKI SLOVAR

- Anonimizacija – izbris osebnih podatkov iz nabora vseh podatkov
- Produkcijsko okolje – okolje, kjer poteka obratovanje informacijskega sistema
- Testno okolje – okolje, kjer se opravljajo testi programske opreme pred sprejemom v obratovanje

1 POLITIKA RAZVOJA, SPREMINJANJA IN VZDRŽEVANJA PROGRAMSKE OPREME

1.1 Namen

Namen dokumenta je opredeliti postopek razvoja in vzdrževanja programske opreme, odgovornosti in naloge sodelujočih, način nadzora ter dokumentacijo, ki jo je potrebno pri tem izdelati.

Namen navodila je zagotoviti, da ima programska oprema izvajalcev zdravstvene dejavnosti zahtevano funkcionalnost, zanesljivost in učinkovitost, da izpolnjuje varnostne zahteve ter da testiranje in vpeljava programske opreme v produkcijsko okolje poteka nadzorovano in ne ovira procesov v produkcijskem okolju oziroma ne vpliva na produkcijske podatke.

1.2 Navodilo za izvajanje razvoja programske opreme, ki ga naročimo pri zunanjem izvajalcu

Razvoj programske opreme je projektno organiziran in se izvaja po predpisanih fazah:

ZAČETEK PROJEKTA IN IZDELAVA PROJEKTNE NALOGE

Izdela se projektna naloga, v kateri se opredeli:

- Poslovne cilje, ki jih bo nova programska oprema izpolnila
- Opis zahtevane funkcionalnosti programske opreme
- Obseg projekta
- Omejitve in predpostavke

IZBIRA IZVAJALCA

Okvir za naročanje storitev pri zunanjih izvajalcih postavlja veljavna zakonodaja.

V razpisni dokumentaciji se pri pogojih, ki jih mora izpolnjevati izvajalec, navede tudi zahteve glede sposobnosti izvajalca, da ustrezno varuje informacije, ki jih izvajalec lahko izkaže s certificiranim sistemom vodenja varovanja informacij ali s kadri s certifikati na področju upravljanja in revidiranja sistemov varovanja informacij.

IMENOVANJE ORGANOV PROJEKTA

Imenuje se:

- projektni svet (zagotavljanje potrebnih virov, sprejemanje odločitev ob kontrolnih točkah in izjemnih situacijah, potrditev prevzemov programske opreme)
- vodjo projekta (planiranje in koordiniranje dela sodelujočih pri izvedbi, vodenje projektne dokumentacije, poročanje projektnemu svetu)
- člane projektne skupine (izvajanje nalog)

IZDELAVA VZPOSTAVITVENEGA DOKUMENTA PROJEKTA

Izdela se vzpostavitveni dokument projekta, ki vsebuje:

Predstavitev projekta

- namen

- cilji
- predpostavke, omejitve, tveganja

Vsebina projekta

- prednosti nove programske opreme
- tehnične lastnosti
- varnostne zahteve

Organizacija projekta

- organizacijska shema in opis zadolžitev sodelujočih
- nadzor projekta: določi se kontrolne točke – preglede terminskega načrta in validacijo razvoja
- informacijska podpora za vodenje projekta

Načrt razvoja:

- izdelki
- terminski načrt z opisom aktivnosti
- plan resursov

POTRDITEV VZPOSTAVITVENEGA DOKUMENTA PROJEKTA

Projektni svet potrdi vzpostavitveni dokument projekta.

IZDELAVA SPECIFIKACIJ

Pripravi se tehnični načrt oziroma specifikacije, v katerih se opredeli:

- potrebne funkcionalnosti
- enolične specifikacije elementov programske opreme
- varnostne zahteve, ki vključujejo, niso pa izključno omejene na:
    - zahteve ob prijavi (uporaba enoličnih identifikatorjev kot to določa Politika nadzora dostopa)
    - funkcionalnosti, ki zagotavljajo varnost podatkov v fazi vnosa, obdelave, prenosa in hranjenja (mehanizmi validacije vhodnih in izhodnih podatkov, šifriranje itd.)
    - zahteve glede revizijskih sledi (opredeljeno v Politiki revizijskih sledi)
- načrt testiranja (priprava običajnih in mejnih testnih primerov)

IZVEDBA RAZVOJA PROGRAMSKE OPREME

Razvoj poteka v razvojnem okolju na računalniški opremi izvajalca, ki je prilagojena zahtevam razvoja. V skladu s Politiko upravljanja kakovosti in varnosti storitev tretjih strank je vodja projekta odgovoren, da izvajalca že pred začetkom razvoja seznani z določili varnostne politike, ki jih je izvajalec dolžan upoštevati.

Vodja projekta spremlja potek razvoja skladno z načrtom projekta ter ob kontrolnih točkah poroča projektnemu svetu. V primeru neskladnosti z načrtom projekta se projektni svet odloča o spremembi načrta, prekinitvi ali nadaljevanju projekta.

IZDELAVA DOKUMENTACIJE

Izdela se dokumentacija nove programske opreme, ki vsebuje vsaj:

- navodilo za namestitev (testne in produkcijske verzije)
- enolično oznaka nove verzije in opis sprememb nove verzije

- opis tehničnih zahtev za strojno in programsko opremo strežnika, na katerem bo nameščena nova programska oprema
- navodilo za testiranje
- uporabniški priročnik

TESTIRANJE

Testiranje programske opreme je obvezna faza pred prevzemom.

Prvo testiranje izvede izvajalec že v svojem razvojnem okolju z namenom odpraviti neskladnosti s specifikacijami programske opreme, ki so opredeljene v pogodbi.

Nadaljnje testiranje izvede izvajalec v testnem okolju organizacije oziroma na testni računalniški opremi, ki mora biti od produkcijskega okolja ločena tako, da testiranje ne more vplivati na produkcijo. Testno okolje je funkcionalno oziroma po zmogljivostih enako produkcijskemu okolju. V ta namen vodja projekta najprej poskrbi, da izvajalec podpiše izjavo o dolžnosti varovanja informacij, nato pa sproži zahtevo za dodelitev dostopa izvajalcu do testnega okolja v omrežju organizacije. Skrbnik testnega sistema pripravi testno okolje in izvajalcu dodeli dostop do testnega sistema v skladu z navedbami v zahtevku za dostop do testnega okolja. Postopek za dodelitev dostopa tretji strani do informacijskega sistema in informacij izvajalca zdravstvene dejavnosti je opredeljen v Politiki upravljanja kakovosti in varnosti storitev tretjih strank. Skrbnik podatkov je odgovoren za pripravo testnih podatkov, ki so anonimizirani oziroma spremenjeni tako, da jih ni več mogoče povezati s posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa. V nabor podatkov se po potrebi vključi podatke, pri katerih je bilo testiranje v preteklosti neuspešno.

Zunanji izvajalec v testnem okolju organizacije testira osnovno funkcionalnost programske opreme v skladu z načrtom testiranja oziroma testnimi primeri, ki so bili opredeljeni v specifikacijah. Rezultate testiranja mora zunanji izvajalec vpisati v zapisnik testiranja. Zapisnik testiranja zunanji izvajalec podpiše in ga posreduje vodji projekta.

Prevzemno testiranje programske opreme izvedejo odgovorne osebe organizacije v testnem okolju. Cilj je ugotoviti vsebinske in tehnične napake aplikacije in potrditi njeno funkcionalnost in zmogljivost v običajnih in mejnih primerih. Z namenom odkriti morebitne ranljivosti programske opreme se izvede še varnostni pregled, s katerim se preveri zagotavljanje zaupnosti, celovitosti, nezmožnosti zanikanja in mehanizme identifikacije. Rezultate testiranja se zapiše v zapisnik testiranja. V primeru ugotovljenih neustreznosti oziroma odstopanj od specifikacij, navedenih v pogodbi, vodja projekta uredi, da zunanji izvajalec napake oziroma odstopanja popravi.

Ko se z ustreznim postopkom testiranja ugotovi, da izdelana programska oprema zagotavlja v pogodbi opredeljeno funkcionalnost, zmogljivost in varnostne zahteve, odgovorne osebe, ki so izvedle testiranja, s podpisom potrdijo zapisnik rezultatov testiranja.

PREVZEM

Za prevzem programske opreme je odgovoren vodja projekta, ki prevzame programsko opremo z ustrezno dokumentacijo ter preveri njeno ustreznost.

Prevzem programske opreme in dokumentacije potrdita vodja projekta in projektni svet s podpisom primopredajnega zapisnika.

NAMESTITEV PROGRAMSKE OPREME

Vodja projekta posreduje zahtevo za namestitev programske opreme v produkcijsko okolje osebi, ki je odgovorna za informacijski sistem. Zahtevi mora priložiti navodila za namestitev, tehnično dokumentacijo, programsko opremo in zapisnik rezultatov testiranja programske opreme.

Namestitev programske opreme v produkcijsko okolje sme opraviti le pooblaščeni sistemski skrbnik programske opreme ali sistema.

UVAJANJE UPORABNIKOV

Izvede se usposabljanje uporabnikov, s katerim se jih usposobi za uporabo nove programske opreme.

1.3 Vzdrževanje programske opreme

V kolikor uporabniki pri delu s programsko opremo naletijo na težave oziroma napake, jih sporočijo na enak način kot vse ostale težave in napake delovanja informacijskega sistema. Pri prijavi napake ali težave mora uporabnik navesti:

- ob kateri akciji 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 vodjo projekta, ki je bil odgovoren za razvoj programske opreme. Vodja projekta ugotovi vzrok za težavo ali napako in po potrebi v reševanje vključi zunanjega izvajalca, ki je razvil programsko opremo. Če je vzrok za težavo ali napako take narave, da zahteva spremembo programske opreme, vodja projekta sproži postopek za razvoj nove verzije, ki se jo testira in vpelje v produkcijo v skladu z navodilom za razvoj programske opreme.

Univerzitetni rehabilitacijski inštitut
Republike Slovenije - **Soča**

Naziv dokumenta:	**POLITIKA NADZORA SPREMEMB INFORMACIJSKEGA SISTEMA (PROGRAMSKE IN SISTEMSKE OPREME TER STROJNE OPREME)**	
Namen dokumenta:	Dokument opisuje pravila in postopke spreminjanja informacijskega sistema	
Številka dokumenta:	**PO 15 POLITIKA NADZORA SPREMEMB INFORMACIJSKEGA SISTEMA**	
Verzija:	**1**	
Stopnja zaupnosti:	**JAVNO**	**Število strani: 4**
Datum odobritve:	**15.7.2015**	Dokument stopi v veljavo v 3 dneh od datuma odobritve.
Referenčni dokument:	**PO 03 Krovna politika varovanja informacij**	

Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.

Pregledal (skrbnik):	**Odobril:**
Vodja I, Vodja službe za informatiko, Inženir tehničnih strok VII/2 (I), Informacijska varnost	Robert Prezelj, u.d.i.e., skrbnik SUIV

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

TERMINOLOŠKI SLOVAR

- Produkcijsko okolje - okolje, kjer poteka obratovanje informacijskega sistema
- Testno okolje - okolje, kjer se opravljajo testi programske opreme 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 najvišjega vodstva organizacije

1 POLITIKA NADZORA SPREMEMB INFORMACIJSKEGA SISTEMA (PROGRAMSKE IN SISTEMSKE OPREME TER STROJNE OPREME)

1.1 Namen

Politika nadzora sprememb informacijskega sistema določa pravila in postopke spreminjanja informacijskega sistema. Pravila in postopki omogočajo natančen potek sprememb informacijskega sistema in nadzor, ki zagotavlja samo odobrene spremembe. Neodobrene spremembe imajo lahko za posledico nedelovanje informacijskega sistema izvajalca zdravstvene dejavnosti, kar lahko povzroči nezmožnost zagotavljanja storitev uporabnikom.

Pravila in postopki nadzora sprememb informacijskega sistema morajo biti usklajeni z varnostnimi zahtevami in hkrati omogočati neovirano izvajanje zdravstvene dejavnosti. Določitev pravil temelji na razvrstitvi informacij, zakonodaji in pogodbenih obveznostih, ki se tičejo zaščite dostopov do informacij in storitev. Politiko nadzora sprememb informacijskega sistema je potrebno pregledovati in prilagajati ob spremembah procesov ter občutljivosti informacij.

1.2 Nabava programske in sistemske opreme ter strojne opreme

Za nabavo morajo izvajalci zdravstvene dejavnosti izdelati predlog s specifikacijami, ki upoštevajo potrebe organizacije. V specifikacijah morata biti natančno določena zahtevana funkcionalnost in zmogljivost opreme, vključene pa morajo biti tudi varnostne zahteve iz Politike razvoja, spreminjanja in vzdrževanja programske opreme.

1.3 Namestitev programske in sistemske opreme ter strojne opreme

Programsko opremo je potrebno pred namestitvijo v produkcijsko okolje ustrezno testirati v testnem okoljem, pri tem pa je pomembno, da se predvidi vse okoliščine, ki se bodo pojavile v produkcijskem okolju. Pred spremembami in migracijami se izdela varnostna kopija sistema, stari sistem se ohrani, da je možna povrnitev v prvotno stanje.

Vsa programska oprema mora ustrezati zahtevam in pogojem licenčnih predpisov.

Skrbniki računalniških sistemov (služba za informatiko, zunanji sodelavci…) so odgovorni za spremljanje veljavnosti oziroma poteka licenc in so dolžni sprožiti postopek za nabavo novih licenc (izda se predlog s specifikacijami za nabavo).

Na računalniški IS je dovoljeno nameščati le odobreno programsko opremo, ki jo določi pooblaščena oseba (služba za informatiko, varnostni inženir itd.). Kakršnokoli nameščanje druge programske opreme brez dovoljenja pooblaščenih oseb (služba za informatiko, varnostni inženir itd.) in mimo postopkov odobritve nove programske opreme je prepovedano.

Namestitev strojne opreme mora biti izvedena s strani pooblaščenih oseb (služba za informatiko, zunanji sodelavci itd.), ki preverijo delovanje sistema po namestitvi. Pred spremembami strojne opreme se izdela varnostna kopija sistema, stari sistem se ohrani, da je možna povrnitev v prvotno stanje. Kakršnekoli spremembe na strojni opremi s strani nepooblaščenih oseb so prepovedane.

Vsa programska in sistemska oprema ter strojna oprema mora biti nameščena s strani pooblaščenih oseb (služba za informatiko, zunanji sodelavci itd.) in usklajena z varnostnimi politikami.

Uporabnike se predhodno obvesti o spremembah informacijskega sistema, ki bi lahko povzročile spremembe pri njihovem rednem delu.

1.4 Nadzor nad verzijami programske opreme

Vsaka spremenjena verzija programske opreme, ki jo nameščamo, mora biti enolično označena, da je zagotovljena sledljivost nad verzijami. Oznako verzije programske opreme določi razvijalec programske opreme. Izvajalec zdravstvene dejavnosti je odgovoren, da se vodi evidenca verzij (pri razvijalcu ali pri izvajalcu zdravstvene dejavnosti).

1.5 Nadzor sprememb informacijskega sistema

Spremembe računalniškega IS se preverja na notranjih presojah, kjer se ugotavlja, ali so bile spremembe primerno vpeljane in zadostujejo primernemu nivoju informacijske varnosti. Izvajalec zdravstvene dejavnosti lahko za preverjanje uporabi mehanizme varnostnih pregledov.

Univerzitetni rehabilitacijski inštitut
Republike Slovenije - Soča

Naziv dokumenta:	**POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO**	
Namen dokumenta:	Dokument opisuje zahteve za zaščito pred zlonamerno programsko opremo	
Številka dokumenta:	**PO 16 POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO**	
Verzija:	**1**	
Stopnja zaupnosti:	**JAVNO**	**Število strani: 3**
Datum odobritve:	**15.7.2015**	Dokument stopi v veljavo v 3 dneh od datuma odobritve.
Referenčni dokument:	**PO 03 Krovna politika varovanja informacij**	
Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.		
Pregledal (skrbnik): Inženir tehničnih strok VII/2 (I), Informacijska varnost	**Odobril:** Robert Prezelj, u.d.i.e., skrbnik SUIV	

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

TERMINOLOŠKI SLOVAR

- Zlonamerna koda – škodljiva programska koda z namenom škodovanja informacijskim sistemom

1 POLITIKA ZAŠČITE PRED ZLONAMERNO PROGRAMSKO OPREMO

1.1 Namen

Namen dokumenta je opredeliti mehanizme za zaščito pred zlonamerno programsko opremo in zmanjšati možnost, da bi le-ta ogrozila neoporečnost in zaupnost informacij in programske opreme.

1.2 Zaščita pred zlonamerno programsko opremo

Da bi komunikacijske segmente omrežja in strežnike zaščitili pred zlonamerno kodo in njenim nenadzorovanim razširjanjem, morajo izvajalci zdravstvene dejavnosti zadostiti sledečim zahtevam:

- Izvajalec zdravstvene dejavnosti mora uporabljati programsko opremo za zaščito pred virusi in drugo neželeno programsko opremo (spyware, adware, grayware itd). Omenjena programska oprema mora biti nameščena na vse odjemalce.
- Uporabljena programska oprema za zaščito pred zlonamerno programsko opremo se mora redno posodabljati, prav tako pa se mora redno izvajati pregledovanje trdih diskov in prenosnih medijev.

Glede na dobro prakso bi izvajalcem zdravstvene dejavnosti priporočali razmejitev lokalnih omrežij oziroma ločitev delov omrežij, v katera so priključeni odjemalci, od delov omrežij, v katere so priključeni strežniki. Prav tako bi izvajalcem priporočali omejitev neposrednih administrativnih dostopov iz uporabniških v strežniške dele omrežja.

Univerzitetni rehabilitacijski inštitut
Republike Slovenije - Soča

Naziv dokumenta:	**POLITIKA UPRAVLJANJA KAKOVOSTI IN VARNOSTI STORITEV TRETJIH STRANK**	
Namen dokumenta:	Dokument opisuje okvir za upravljanje kakovosti storitev tretjih strank	
Številka dokumenta:	**PO 17 POLITIKA UPRAVLJANJA KAKOVOSTI IN VARNOSTI STORITEV TRETJIH STRANK**	
Verzija:	**1**	
Stopnja zaupnosti:	**JAVNO**	**Število strani: 6**
Datum odobritve:	**15.7.2015**	Dokument stopi v veljavo v 3 dneh od datuma odobritve.
Referenčni dokument:	**PO 03 Krovna politika varovanja informacij**	
Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.		
Pregledal (skrbnik): Vodja I, Vodja službe za informatiko	**Odobril:** Robert Prezelj, u.d.i.e., skrbnik SUIV	

Univerzitetni rehabilitacijski inštitut Republike Slovenije - Soča, Linhartova 51, 1000 Ljubljana
Tel: +386 (0) 1 475 81 00
E-pošta: info@ir-rs.si
http://www.ir-rs.si/

TERMINOLOŠKI SLOVAR

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

1. POLITIKA UPRAVLJANJA KAKOVOSTI IN VARNOSTI STORITEV TRETJIH STRANK

1.1 Namen

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

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

1.2 Pogodbeno urejanje razmerij s tretjimi strankami

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

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

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

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

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

- način poročanja ter obveščanja o varnostnih incidentih**,**
- postopke za zaščito sredstev za izvajanje storitev,
- zahteve glede varovanja podatkov izvajalca zdravstvene dejavnosti,
- nadzor dostopa, vključno z dovoljenimi metodami dostopa tretje stranke,
- vodenje in dostopnost seznama izvajalcev, pooblaščenih za izvajanje storitev,
- obveznosti glede namestitve in vzdrževanja strojne in programske opreme tretje stranke ter zahtevanih fizičnih in logičnih nadzornih mehanizmov dostopa do sistemov, storitev in informacij,
- zahteve, da tretja stranka omrežje varuje pred grožnjami iz zunanjih omrežij z opremo, ki zagotavlja največjo možno varnost pred zlonamerno programsko opremo in zunanjimi vdori do sistemov, storitev in podatkov,

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

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

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

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

1.3 Upravljanje sprememb pogodbenih storitev tretjih strank

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

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

1.4 Politika nadzora dostopa tretjih strank do informacijskega sistema in informacij

Ko se pojavi potreba po dostopu tretjih strank do informacij ali informacijskega sistema izvajalca zdravstvene dejavnosti, se najprej izvede analizo tveganja in ugotovi potrebne varnostne ukrepe. Dostop tretjim strankam do informacij in informacijskega sistema ni dovoljen, dokler niso implementirani ustrezni varnostni in nadzorni mehanizmi in niso stopila v veljavo potrebna interna pravila in pogodba, ki definira pogoje dostopa.

Pravila za določanje dostopov opisujejo načine dostopa in omogočajo nadzor nad dostopi do informacij in informacijskega sistema. Pravila morajo vedno odražati poslovne potrebe

izvajalca zdravstvene dejavnosti in s tem povezane varnostne zahteve. Osnova za izdelavo pravil je varnostna razvrstitev podatkov, ki jo določa Politika o navodilih za klasifikacijo, označevanje in ravnanje z informacijami.

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

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

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

1.4.1 Logični dostop do informacijskega sistema in informacij

Za odobritev in izvedbo postopka za dostop v omrežje za tretje stranke je potrebno pripraviti zahtevek ali izdelati drug dokument, ki vsebuje vse predpisane podatke. Zahtevek za zunanjega sodelavca izpolni vodja službe za informatiko.

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

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

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

- Odgovorna oseba za informacijski sistem pregleda zahtevek in dopolni parametre obrazca.
- Priporočljivo je, da se za dostop tretjih strank glede na ocenjeno stopnjo tveganja pripravijo ločeni segmenti omrežja, ki so povezani z omrežjem izvajalca zdravstvene dejavnosti preko požarne pregrade.
- Tretji stranki se omogoči dostop le do tistih servisov, ki so potrebni za delo tretje stranke – v skladu z odobrenim zahtevkom.
- Določi se gesla za dostop do notranjih mrežnih virov za tretjo stranko – v skladu z odobrenim zahtevkom.

- Sistemski skrbnik izvajalca zdravstvene dejavnosti izvede test dostopa.
- Tretja stranka podpiše zahtevek za dostop in s tem potrdi prevzem gesel ter seznanjenost z varnostnimi pravili dostopa.
- Zahtevek se arhivira na ustrezno mesto.

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

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

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

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

1.4.2 Fizični dostop do sistemov

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

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

Izvajalec zdravstvene dejavnosti je odgovoren 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 pooblaščenim osebam. Incidente je potrebno skladno z varnostno politiko identificirati in reševati glede na kritičnost posameznega incidenta.

Dokument predstavlja okvir za upravljanje incidentov. Namen dokumenta je opredeliti postopke, s katerimi organizacija zagotovi, da se incidenti obvladujejo, oziroma da se odpravijo ali zmanjšajo posledice incidenta.