**Univerzitetni rehabilitacijski inštitut**  
*Republike Slovenije - Soča*

<table>
<thead>
<tr>
<th>Naziv dokumenta:</th>
<th>KROVNA POLITIKA VAROVANJA INFORMACIJ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Namen dokumenta:</td>
<td>Dokument opisuje cilje varovanja informacij v URI - Soča</td>
</tr>
<tr>
<td>Številka dokumenta:</td>
<td>PO 03 KROVNA POLITIKA VAROVANJA INFORMACIJ</td>
</tr>
<tr>
<td>Verzija:</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stopnja zaupnosti:</th>
<th>JAVNO</th>
<th>Število strani:</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datum odobritve:</td>
<td>15.12.2014</td>
<td>Dokument stopi v veljavo v 8 dneh od datuma odobritve.</td>
<td></td>
</tr>
</tbody>
</table>

Referenčni dokument:
- Zakon o varstvu dokumentarnega in arhivskega građiva ter arhivih (ZVDAGA)
- Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP)
- Zakon o varstvu osebnih podatkov (ZVOP-1)
- Zakon o dostopu do informacij javnega značaja (ZVDIJZ)
- Zakon o zavodih (ZZ)
- Zakon o zdravstveni dejavnosti (ZZDej)
- Uredba o varstvu dokumentarnega in arhivskega građiva
- Enotne tehnološke zahteve 2.1
- Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje
- ISO/IEC 27001:2013

Dokument je namenjen seznanitvi zaposlenih, pogodbenih sodelavcev in odjemalcev inštituta in vsebuje javno dostopne informacije.
<table>
<thead>
<tr>
<th>Pregledal (skrbnik):</th>
<th>Odobril (varnostni forum – odbor za kakovost):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robert Prezelj, u.d.i.e.</td>
<td>Generalni direktor inštituta:</td>
</tr>
<tr>
<td></td>
<td>mag. Robert Cugelj</td>
</tr>
<tr>
<td></td>
<td>Strokovna direktorica inštituta:</td>
</tr>
<tr>
<td></td>
<td>prof. dr. Helena Burger, dr. med</td>
</tr>
<tr>
<td></td>
<td>Pomočnica gen. dir. za zdravstveno nego:</td>
</tr>
<tr>
<td></td>
<td>Ksenija Karan, dipl. med. ses.</td>
</tr>
</tbody>
</table>

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/](http://www.ir-rs.si/)

stran 2 od 7
1. Namen krovne in področnih politik varovanja informacij


Cilj varovanja informacij je preprečevati oziroma zmanjšati posledice varnostnih incidentov na najmanjšo možno mero. Namen varnostne politike je ugotoviti pomembnost informacij za poslovanje inštituta s stališča:

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

Varnostni incident je vsak dogodek, ki pomeni implicitno ali eksplicitno kršitev varnostne politike in povečuje tveganje zaupnosti, celovitosti ali razpoložljivosti informacij inštituta.

Krovna in področne politike varovanja informacij določajo varnostne ukrepe in postopke v skladu z varnostno občutljivostjo, poslovno vrednostjo in kritičnostjo informacij, ne glede na obliko, v kateri se informacije pojavljujo: na računalnikih, na papirju ali na prenosnih pomnilniških medijih ter pri prenosu preko omrežja oziroma pri ustnem posredovanju.

Zaradi vse večje odvisnosti poslovanja od informacijske tehnologije se povečuje različnost različne zunanje in notranje grožnje, ki postajajo čedalje bolj razširjene in učinkovite pri povzročanju škode inštitutu. Krovna politika varovanja informacij s pomočjo varnostnih kontrolov postavi celovit okvir za zagotavljanje varovanja informacij in informacijskega sistema.

2. Obseg politike varovanja informacij

Politike, navodila in postopki varovanja informacij na nižjem nivoju pokrivajo vse z informacijami povezane poslovne procese inštituta. Za vsa področja varovanja informacij so določeni varnostni postopki, organizacijski predpisi in delovna navodila, ki določajo, kako zaščititi informacijsko premoženje.


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

1) **Informacijske varnostne politike**
   Zagotoviti usmeritve vodstva in njegovo podporo informacijski varnosti v skladu s poslovnimi zahtevami ter ustreznimi zakoni in predpisi.

2) **Organiziranje informacijske varnosti**
   Vzpostaviti okvir upravljanja za začetek in kontrolo izvajanja ter delovanja informacijske varnosti v organizaciji.

3) **Varnost človeških virov**
   Zagotoviti, da zaposleni in pogodbeniki razumejo svoje odgovornosti in imajo ustreze kompetence za naloge, ki jih opravljajo v okviru SUIV, da se zaposleni in pogodbeniki zavedajo svojih odgovornosti na področju informacijske varnosti ter jih izpolnjujejo. Zaščititi je potrebno interese organizacije v okviru procesa prekinitve ali spremembe zaposlitve.

4) **Upravljanje dobrin**
   Opredeliti organizacijske dobrine in določiti ustreze odgovornosti na področju zaščite, zagotoviti, da informacije prejmejo ustrezen raven zaščite v skladu z njihovim pomenom za organizacijo, prepričiti nepooblaščeno razkritje, spreminjanje, odstranitev ali uničenje informacij.

5) **Nadzor dostopa**
   Omogočiti dostop do informacij in naprav za obdelavo informacij, zagotoviti pooblaščen uporabniški dostop in prepričiti nepooblaščen dostop do sistemov, storitev in aplikacij, doseči odgovornost uporabnikov za zaščito svojih informacij za preverjanje verodostojnosti.

6) **Kriptografija**
   Zagotoviti ustrezen in uspešno uporabo kriptografije za zaščito zaupnosti, verodostojnosti in/ali celovitosti informacij.

7) **Fizična in okoljska varnost**
   Prepričiti nepooblaščen fizični dostop, poškodbe in poseganje v informacije ter naprave za obdelavo informacij organizacije, prepričiti izgube, poškodbe, kraje ali zlorabe dobrin in prekinitve operacij organizacije.

8) **Varnost operacij**
Zagotoviti pravilno in varno delovanje naprav za obdelavo informacij, da so informacije in naprave za obdelavo informacij zaščitene pred zlonamerno programsko opremo, ustrezno zaščito pred izgubo podatkov, beležiti dogodke in ustvarjati dokaze, zagotoviti celovitost operativnih sistemov, preprečiti izkoriščanje tehničnih ranljivosti in zmanjšati vpliv dejavnosti presoje na operativne sisteme.

9) Varnost komunikacije
Zagotoviti zaščito informacij v omrežjih in zaščito podpornih naprav za obdelavo informacij ter vzdrževati varnost informacij, ki se prenašajo znotraj organizacije in s katerim koli zunanjim subjektom.

10) Pridobivanje, razvoj in vzdrževanje sistemov
Zagotoviti, da je informacijska varnost sestavni del informacijskih sistemov v celotnem življenjskem ciklu, da se informacijska varnost načrtuje in izvaja v okviru razvojnega življenjskega cikla informacijskih sistemov ter zagotoviti zaščito podatkov, ki se uporabljajo za testiranje.

11) Odnosi z dobavitelji
Zagotoviti zaščito dobrin organizacije, ki so dostopne dobaviteljem ter vzdrževati dogovorjeno raven informacijske varnosti in izvajanja storitev v skladu z dobaviteljem.

12) Upravljanje informacijskih varnostnih incidentov
Zagotoviti uporabo doslednega in uspešnega pristopa k upravljanju informacijskih varnostnih incidentov, vključno s sporočanjem o varnostnih dogodkih in slabostih.

13) Vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja
Neprekinjena informacijska varnost mora biti vključena v sisteme upravljanja neprekinjenega poslovanja organizacije, zagotoviti je potrebno razpoložljivost naprav za obdelavo informacij.

14) Skladnost
Preprečiti kršitve pravnih obveznosti, predpisov, zakonskih ali pogodbenih obveznosti v zvezi z informacijsko varnostjo ter kakršnih koli varnostnih zahtev ter zagotoviti izvajanje in upravljanje informacijske varnosti v skladu z organizacijskimi varnostnimi politikami in postopki.

3. Splošna odgovornost in odgovornost za posamezna področja varovanja informacij
Vodstvo inštituta je odgovorno za vzpostavitev SUIV, za spremljanje in nadziranje učinkovitosti varnostnih ukrepov in postopkov.

Za upoštevanje in izvajanje posameznih varnostnih ukrepov in postopkov so zadolženi vsi zaposleni, vodstvo inštituta pa je odgovorno za izvajanje politike varovanja informacij v celoti in za zagotovitev potrebnih finančnih in človeških virov.


Delo skrbnika SUIV določa in nadzira Varnostni forum, ki je sestavljen iz članov kolegija generalnega direktorja inštituta. Zaradi usklajenosti s sistemom kakovosti naloge Varnostnega stran 5 od 7
foruma prevzame Odbor za kakovost, ki ga sestavljajo generalni direktor inštituta, strokovna
direktorica in pomočnica generalnega direktorja za zdravstveno nego.

Naloga Varnostnega foruma je:

- zagotavljanje virov in potrjevanje ukrepov, ki zagotavljajo primerno varovanje
  informacij.

Naloge skrbnika SUIV so:

- opredelitev obsega in mej SUIV z vidika značilnosti poslovanja, organizacije, lokacije
  ter zahtev zakonodaje s področja varovanja podatkov,
- nadziranje in zaščita dokumentov politike varovanja informacij in postopki pri
  spremembah dokumentacije,
- priprava navodila za izvajanje ocene tveganja,
- najmanj enkrat letno oceniti varnostna tveganja,
- najmanj enkrat letno pripraviti poročilo ocene tveganja in načrta za obravnavo tveganj,
- najmanj enkrat letno izvesti notranjo presojo in pripraviti zapisnik notranje presoje,
- zagotavljanje ozaveščenosti zaposlenih glede varovanja informacij ter uskretnje
  usposobljenosti, da razumejo varnostno politiko in ukrepe,
- komuniciranje s pogodbenimi sodelavci in vsemi uporabniki informacij in
  informacijskega sistema v zadevah, ki se nanašajo na SUIV,
- upravljanje z varnostnimi incidenti in varnostnimi pomanjkljivostmi,
- izvedba varnostnih ukrepov za izboljšanje stanja varovanja informacij.

4. Odgovornosti pri poročanju incidentov in varnostnih pomanjkljivosti

V proces stalnega izboljševanja nivoa varnosti informacij in informacijskih sredstev morajo
biti vključeni vsi zaposleni in pogodbeni sodelavci. Naloga skrbnika SUIV je, da zaposlene in
pogodbene sodelavce ustrezo seznanit z varnostnimi zahtevami in kontrolami ter jih usposobi
za varno uporabo informacij in informacijskega sistema.

Zaposleni in pogodbeni sodelavci morajo sporočiti opažene varnostne incidente, kot so:

- varnostne pomanjkljivosti,
- nepravilno ali sumljivo delovanje informacijskih sistemov,
- nedelovanje sistemov,
- kršitve določil SUIV.

Skrbnik SUIV zbira prijave varnostnih incidentov, jih pregleduje in analizira, obvesti
Varnostni forum ter na incidente odgovori z ustreznimi ukrepi. O incidentih in ukrepih se vodi
zapise ter se jih predstavi na sestankih Varnostnega foruma in vodstvenem pregledu.
5. Vzdrževanje politike varovanja informacij

Ob spremembah zakonodaje, pojavu novih groženj, novih varnostnih incidentov, spremembah organizacijske ali tehnične infrastrukture, ki vplivajo na varovanje informacij in informacijskih sistemov, se bo SUIV nenehno prilagajal z uvajanjem novih in dopolnjevanjem že obstoječih varnostnih ukrepov in postopkov. Dinamično prilagajanje politike varovanja informacij v skladu z zahtevami in spremembami inštituta, ki vplivajo na oceno varnostnega tveganja, je zadolžitev odgovornega za varovanje informacij.

6. Upravljanje z dokumenti politike varovanja informacij

Dokumenti politike varovanja informacij so objavljeni skladno z določili sistema kakovosti na način, da so dostopni zaposlenim, pogodbenim sodelavcem in vsem uporabnikom informacij in informacijskega sistema inštituta. Vsak dokument politike varovanja informacij ima skrbnika, ki je zadolžen za njegovo pravočasno obnavljanje in spreminjanje ter lastnika, ki dokument odobri.

Dopolnitev ali izboljšavo dokumenta lahko predlaga vsak zaposleni ali pogodbeni sodelavec, tako da predlog naslovi na skrbnika. Ko so dokumenti spremenjeni in odobreni, jih je potrebno objaviti ter zamenjati staro verzijo. O spremembi je potrebno obvestiti zaposlene, pogodbene sodelavce in vse uporabnike informacij in informacijskega sistema, ki jih morajo upoštevati pri svojem delu.

7. Sankcije

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