Uprava
Univerze v Ljubljani

Univerza *v Ljubljani*

p.p.362, Kongresni trg 12
1001 Ljubljana, Slovenia
telefon: 01 241 85 00
faks: 01 241 86 60
rektorat@uni-lj.si
www.uni-lj.si

KROVNA POLITIKA INFORMACIJSKE VARNOSTI UNIVERZE V LJUBLJANI

Datum: 8. 11. 2018
Avtor: Univerzitetna služba za informatiko
Verzija: 1.0
Klasifikacija: javno

Univerza *v Ljubljani*
Podpisnik: rektor UL
Izdajatelj: SIGEN-CA G2
Številka certifikata: 578E69020000000057205FC9
Potek veljavnosti: 03. 10. 2022
Čas podpisa: 03. 07. 2020 17:31

Splošne določbe:

1. Namen dokumenta: Zagotoviti skladnost z načeli zaupnosti, celovitosti in razpoložljivosti
2. Vsebina: Krovna politika informacijske varnosti
3. Lastnik: Univerza v Ljubljani
4. Avtor: Univerzitetna služba za informatiko
5. Skrbnik dokumenta: Skrbnik informacijske varnosti
6. Zgodovina različic:

Različica	Datum zadnje spremembe	Izvedene spremembe
1.0	8. 11. 2018	Vzpostavitev dokumenta

7. Odobril:

Ime in priimek	Datum odobritve	Podpis
prof. dr. Igor Papič, rektor Univerze v Ljubljani	10. 3. 2020	

KAZALO

1 UVOD

Univerza v Ljubljani (v nadaljevanju UL) kot najstarejša in največja visokošolska in znanstveno raziskovalna ustanova v Republiki Sloveniji je zavezana k etičnemu, pravnemu in poslovnemu ravnanju z informacijami, s katerimi razpolaga tako, da zagotovi skladnost z načeli zaupnosti, celovitosti in razpoložljivosti. UL zagotavlja, da so vse informacije točne, pravočasne, na voljo samo tistim osebam, ki imajo ustrezna pooblastila za dostop do njih in zaščitene pred nepooblaščenim razkritjem.

Z namenom izvajanja teh načel vodstvo UL sprejema Krovno politiko informacijske varnosti na UL (v nadaljevanju Krovna politika), ki velja za vse zaposlene, pogodbene izvajalce, študente in druge osebe (v nadaljevanju uporabniki) na rektoratu, članicah UL (v nadaljevanju pristopnice UL) in pridruženih članicah UL, ki ta dokument sprejmejo, uvrstijo v svoje interne akte in ga izvajajo. Uporabniki morajo biti seznanjeni z vsebino Krovne politike in podrejenega dokumenta Politike informacijske varnosti.

Ostali uporabljeni izrazi so opredeljeni v Politiki informacijske varnosti v poglavju 1 Slovar izrazov.

2 PREDMET UREJANJA IN PODROČJE UPORABE

S tem dokumentom in podrejeno dokumentacijo se določajo organizacijski, tehnični in logično-tehnični postopki in ukrepi glede delovanja in vzdrževanja SUVI.

Vsa informacijska sredstva in viri UL (v nadaljevanju informacijska sredstva) morajo biti ustrezno zaščiteni, zlasti pred kršitvijo zakonodaje in internimi pravnimi akti, krajo, izgubo, uničenjem, nepooblaščenim dostopom in/ali spremembo. Vsako kompromitiranje ali izguba poslovnih informacij ima lahko velik vpliv na UL, skladnost z zakonodajo, celovitost ter zaupanje v UL kot celoto.

Informacije po ISO/IEC 27000 so vsa informacijska sredstva, ki so tako kot druga pomembna poslovna sredstva, bistvena za poslovanje UL, zato jih je treba ustrezno varovati. Slednje velja za vsa informacijska sredstva, ki so v lasti ali najemu UL. Informacije so v različnih oblikah: digitalna oblika (npr. podatkovne datoteke, shranjene na elektronskih ali optičnih medijih), materialna oblika (npr. na papirju), kot tudi nezadostne informacije v obliki znanja zaposlenih, ki se lahko prenašajo preko kurirja, z elektronsko ali verbalno komunikacijo.

UL je pripravila enotno in notranje usklajeno Krovno politiko in vse njej podrejene dokumente (Politika informacijske varnosti in Operativna navodila). Podrejeni dokumenti se lahko uporabljajo nespremenjeno ali z uredniškimi spremembami, pri čemer morajo pristopnice in pridružene članice UL zagotavljati skladnost in ustreznost prilagojenih podrejenih dokumentov. Pri razvoju teh dokumentov si bo UL prizadevala zagotavljati ustrezno kontinuiteto in skladnost z zahtevami področne zakonodaje in standarda ISO/IEC 27001.

Krovna politika je sprejeta z dnem, ko jo odobri rektor UL in začne veljati naslednji dan. Krovna politika je objavljena na spletnih straneh UL in je na voljo vsem uporabnikom.

3 NAMEN IN CILJ

Namen Krovne politike je zagotoviti primeren in enovit sistem vodenja, kontrole in varovanja informacijskih sredstev na UL. Glavna naloga SUVI je uspešna in učinkovita zaščita zaupnosti, celovitosti in razpoložljivosti podatkov, informacij ter podporne informacijske tehnologije pred grožnjami in tveganji v zvezi z razkritjem, uničenjem, spreminjanjem in krajo informacij s strani notranjih uporabnikov ali zunanjih oseb ter pred naravnimi in drugimi nesrečami.

UL s tem dokumentom vzpostavlja enotno politiko na področju informacijske varnosti, s katero vzdržuje in nenehno izboljšuje SUVI.

Cilji Krovne politike so:

1. Zagotavljati okvir za določanje ustrezne ravni varovanja informacij za vsa informacijska sredstva in preprečitev oziroma učinkovito in uspešno obvladovanje tveganj, povezana s krajo, razkritjem, uničenjem, nepooblaščenim dostopom, spreminjanjem, izgubo, zlorabo in škodo teh sredstev;
2. Vzpostaviti in spremljati informacijska tveganja ter zagotavljati, da so vsa pod sprejemljivo ravnijo tveganj UL;
3. Nenehno izpopolnjevati SUVI, zlasti na naslednje načine:
    - Dvigovati ozaveščenost in kompetentnost vseh uporabnikov informacijskih sredstev, s seznanjanjem področne zakonodaje, z internimi pravilniki in politikami ter prizadevati si za njihovo izvajanje. Uspešnost seznanjanja in doseganja primerne ravni ozaveščenosti se izvaja skladno s Politiko varovanja človeških virov;
    - Prizadevati si, da vsi uporabniki informacijskih sredstev so seznanjeni in se zavedajo svoje odgovornosti za zaščito zaupnosti, celovitosti in razpoložljivosti informacij: odgovornost za upoštevanje zahtev informacijske varnosti nosi vsak uporabnik sam v skladu s obveznostmi iz delovnega razmerja;
    - Spremljati (neželene) dogodke s področja varovanja informacij, tako da se povečuje varnost celotne UL s preprečevanjem ponavljajočih se dogodkov in s preventivnimi ukrepi proti novim (neželenim) dogodkom, na način, da se preprečuje verjetnost za njihov nastanek ali njihove posledice;
    - Spremljanje rezultatov SUVI in njeno dokumentiranje, ki ga izvaja Skrbnik informacijske varnosti na rektoratu in/ali pristopnicah UL ter vsaj enkrat letno o ugotovljenih rezultatih poroča Varnostnemu forumu. Pregled se opravi pred vsakim vodstvenim pregledom;
    - Vrednotiti SUVI, spremljati rezultate notranjih presoj, napovedati uspešno delovanje SUVI, ki se izvaja z zmanjševanjem števila korektivnih ukrepov in večati število priporočil.
4. Ščititi UL pred namerno ali nenamerno škodljivo uporabo informacijskih sredstev;
5. Zagotavljati varno in neprekinjeno varovanje informacijskih sredstev v skladu s poslovnimi zahtevami ter omejevanje poslovne škode na sprejemljivi ravni s preprečevanjem in zmanjševanjem učinkov varnostnih incidentov.

Krovna politika je skladna z zahtevami veljavnih predpisov s področja varovanja podatkov in zahtevami standarda ISO/IEC 27001:2013.

4 ODGOVORNOSTI

Vsi uporabniki, ki imajo kakršne koli stike z informacijskimi sredstvi, so odgovorni za upoštevanje in izvajanje Krovne politike. Z vsebino Krovne politike in Politike informacijske varnosti so seznanjeni vsi uporabniki, ki so zavezani k doslednemu upoštevanju in izvajanju zahtev in priporočil.

Zaposlene in pogodbene izvajalce se k varovanju informacij lahko zaveže tudi pisno s podpisom ustrezne izjave. Pred podpisom vodstvo seznani uporabnike z vzpostavljeno Krovno politiko in njej podrejene dokumente ter postopki, ki jih zahtevajo, ter relevantnimi pravilniki.

4.1 Odgovornost vodstva

Vodstvo UL s tem dokumentom določa in vzpostavlja Krovno politiko, na podlagi katere vzpostavlja in vzdržuje SUVI. Vodstvo se z njo zavezuje, da bo zagotovilo potrebne finančne in človeške vire ter nudilo

potrebno vsestransko podporo pri vzpostavitvi in vzdrževanju SUVI na UL. Vodstvo UL se zaveda, da je za uspešnost delovanja odvisno od pravilnih, kakovostnih, pravočasnih in dostopnih informacij.

Vodstvo in vsi zaposleni na rektoratu, pristopnicah in pridruženih članicah UL so zavezani k varovanju informacijskih sredstev, skladno z zahtevami Krovne politike in Politike informacijske varnosti s pripadajočimi Operativnimi pravili.

Rektorat, pristopnice[1] in pridružene članice UL morajo:
- Oceniti vrednost svojih informacijskih sredstev ter med njimi prepoznati kritična informacijska sredstva;
- Oceniti tveganja v primeru, da je informacijsko sredstvo izgubljeno, ukradeno, spremenjeno, uničeno ali nedostopno;
- Vpeljati primeren vodstveni nadzor in procese, ki bodo zagotovili neprekinjeno varnost informacijskih sredstev UL, skladno s področno zakonodajo.

Vodstvo UL ima v sklopu vpeljave Krovne politike zlasti naslednje naloge:
- Pregledati in odobriti Krovno politiko ter njene spremembe in dopolnitve;
- Pregledati in potrditi strateške usmeritve na področju informacijske varnosti;
- Zagotoviti potrebne vire in pogoje za izvedbo in izpolnjevanje zahtev SUVI skladno s postavljenimi cilji;
- Določiti vloge in odgovornosti za izvedbo načrta aktivnosti za zmanjšanje tveganj v skladu z oceno tveganj ter pregled meritev učinkovitosti vzpostavljenih ukrepov;
- Odobriti sprejemljivo raven tveganj informacijske varnosti;
- Odobriti pogostost in način izvajanja presoj na področju varovanja informacij;
- Odločiti o ukrepih in aktivnostih pri večjih varnostnih incidentih;
- Spodbujati pomembnost izpolnjevanja zahtev zakonodaje, Krovne politike in pripadajočih dokumentov;
- Preverjati učinkovitost delovanja SUVI na podlagi rezultatov ocen tveganj, notranjih presoj ter vodstvenih pregledov.

4.2 Vloga Varnostnega foruma

Vodstvo je najvišji odločitveni organ SUVI, ki svoje poslanstvo uresničuje tudi skozi delovanje Varnostnega foruma. Slednji sprejema pomembne odločitve s področja varovanja informacij – zlasti predlaga dopolnitve in spremembe ter spremlja izvajanja Krovne politike in pripadajoče dokumentacije.

Vodstvo UL s pisnim sklepom imenuje člane Varnostnega foruma. Člani varnostnega foruma so: glavni tajnik, pomočnik glavnega tajnika za področje informatike, pooblaščena oseba za varstvo osebnih podatkov in skrbnik informacijske varnosti. Vodstvo lahko v Varnostni forum imenuje tudi ostale strokovnjake iz obravnavanega področja.

Naloge Varnostnega foruma za informacijsko varnost so sledeče:
- Vzdrževanje Krovne politike in pripadajoče dokumentacije;
- Predlaganje sprejemljive ravni tveganj;
- Postavljanje prioritet za izvajanje letnega načrta s področja varovanja informacij;
- Določanje nalog in odgovornosti v zvezi z varovanjem informacij;
- Ozaveščanje in izobraževanje uporabnikov;
- Pregledovanje in odobritev rezultatov ocen tveganj s področja varovanja informacij;

[1] Pristopnice so vse organizacijske enote članice UL, ki pristopajo k izvajanju Krovne politike.

- Pregledovanje, odobritev in spremljanje presoj SUVI;
- Sprejemanje usmeritev za izvajanje aktivnosti pri varnostnih incidentih.

4.3 Vloga Skrbnika informacijske varnosti

Vodstvo rektorata pooblasti Skrbnika informacijske varnosti, ki skrbi za izvajanje in nadzor nad SUVI.

Vodstvo pristopnic UL in pridruženih članic UL lahko po lastni presoji pooblasti na nivoju pristopnice UL ali pridružene članice svojega Skrbnika informacijske varnosti, ki skrbi za izvajanje in nadzor nad SUVI na pristopnici UL ali pridruženi članici UL.

Skrbnik informacijske varnosti je neposredno podrejen najvišjemu vodstvu in je vezni člen med uporabniki in Varnostnim forumom.

Skrbnik informacijske varnosti ima naslednje naloge:
- Vodi in koordinira aktivnosti za vzpostavitev in vzdrževanje SUVI;
- Pripravi, pregleda, koordinira in izvaja nadzor nad izvajanjem Krovne politike, Politike informacijske varnosti in druge pripadajoče dokumentacije;
- Posreduje Krovno politiko in Politiko informacijske varnosti v potrditev vodstvu;
- uvaja, izvaja, implementira, administrira in interpretira politike, standarde, napotke in postopke v zvezi z informacijsko varnostjo;
- Organizira in vodi postopek ocene tveganj za pomembne informacijske vire;
- Spremlja, poroča in upravlja varnostne incidente;
- Predlaga Varnostnemu forumu nujne spremembe SUVI;
- Nadzor kršitev in priprava predlogov za preventivno ukrepanje za zmanjševanje kršitev na področju varnosti;
- Aktivno sodeluje na področju varovanja osebnih podatkov in morebitnimi incidenti s pooblaščeno osebo za varovanje osebnih podatkov;
- Organizira interna izobraževanja s področja varovanja informacij in aktivno vključevanje uporabnikov v procese varovanja informacij;
- Sodeluje pri presojah SUVI;
- Sodeluje z zunanjimi strokovnjaki in organizacijami v zvezi z aktivnostmi, povezanimi z varovanjem informacij;
- Vodi preiskave o vseh domnevnih incidentih, prekrških in izrednih dogodkih, ki so vezani na informacijsko varnost;
- Izvaja nadzor nad sistemi dodeljevanja dostopnih pravic uporabnikov do podatkov in sistemov;
- Najmanj enkrat letno izvesti notranjo presojo in pripraviti zapisnik notranje presoje;
- Najmanj enkrat letno izvesti vodstveni pregled in pripraviti zapisnik vodstvenega pregleda ter ga posredovati v potrditev vodstvu.

Odgovoren je za preverjanje skladnosti in izvajanje politik varovanja informacij s Krovno politiko. Skrbnik mora najmanj enkrat letno oziroma skladno z oceno tveganj izvesti notranji pregled nad izvajanjem politike informacijske varnosti. Po notranjem pregledu izdela poročilo z ugotovitvami pomanjkljivosti in predlogi za njihovo odpravo oziroma zmanjšanje, ki ga predstavi vodstvu.

4.4 Odgovornost vseh zaposlenih

Vsi uporabniki, ki uporabljajo informacijska sredstva pri opravljanju obveznosti iz delovnega razmerja, upoštevajo in delujejo v skladu s Krovno politiko. Vodstvo pristopnice UL in pridružene članice UL lahko sprejmejo še ostale varnostne politike na podlagi tega dokumenta.

Uporabniki varnostne incidente, ki jih opazijo, javljajo Skrbniku informacijske varnosti, ki ravna skladno z Operativnim navodilom za upravljanje z varnostnimi incidenti.

UL v internih aktih opredeljuje tudi potrebne aktivnosti za zagotovitev varnostne ozaveščenosti in izvajanje varnostne politike.

Aktivnosti se izvajajo:
- Ob zaposlitvi v smislu seznanjanja in obveze novega sodelavca glede izvajanja varnostne politike ter določanja potrebnega dostopa do informacij;
- V času zaposlitve v smislu izobraževanja, obveščanja in izvajanja sprememb dostopa do informacij;
- Ob prekinitvi zaposlitve v smislu odvzema pravic dostopa do informacij in vrnitve informacijskih virov.

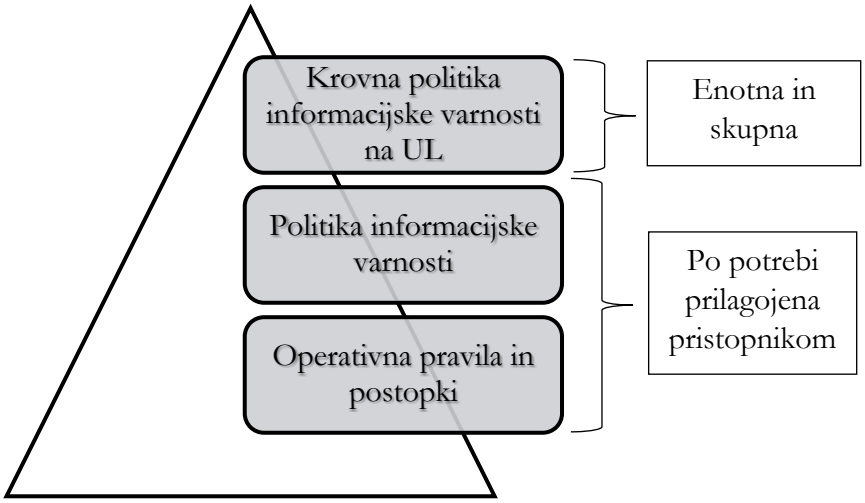
5 STRUKTURA DOKUMENTACIJE VARNOSTNE POLITIKE

Na podlagi Krovne politike vodstvo rektorata UL, vodstvo posamezne pristopnice UL in vodstvo pridružene članice UL sprejme Politike informacijske varnosti ter drugo pripadajočo dokumentacijo, ki vključuje zahteve ter priporočila standarda ISO/IEC 27001:2013.

Politika informacijske varnosti naj vsebuje vsaj minimalni nabor naslednjih vsebin:
- Politika varovanja informacij,
- Organizacija varovanja informacij,
- Varnost človeških virov,
- Upravljanje dobrin,
- Nadzor dostopa,
- Kriptografija,
- Fizična in okoljska varnost,
- Varnost operacij,
- Varnost komunikacije,
- Pridobivanje razvoj in vzdrževanje sistemov,
- Odnosi z dobavitelji,
- Upravljanje informacijskih varnostnih incidentov,
- Vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja,
- Skladnost.

Rektorat, pristopnica UL ali pridružena članica lahko v lastno Politike informacijske varnosti vključijo tudi dodatna poglavja za posamezno področje po lastni presoji.

Na podlagi Politike informacijske varnosti lahko rektorat, pristopnica UL ali pridružena članica sprejme Operativna navodila za operativno izvajanje Politike informacijske varnosti in Krovne politike.



Slika 1: Hierarhija dokumentov

Krovna politika je dostopna tukaj.

Politika informacijske varnosti je dostopna tukaj.

Operativna navodila so dostopna tukaj.

5.1 Predlogi za spremembo in dopolnitev

Predlog za spremembo in dopolnitev lahko poda Skrbnik informacijske varnosti in vsak uporabnik. Utemeljene predloge za spremembo in dopolnitev Krovne politike in pripadajoče dokumentacije obravnava Varnostni forum, ki predlog sprejeme ali zavrne. V primeru zavrnitve predloga Varnostni forum poda obrazložitev z razlogi za zavrnitev in postopek se zaključi. Če je predlog sprejet, mora Skrbnik informacijske varnosti v razumnem roku besedilo Krovne politike in/ali pripadajoče dokumentacije popraviti oziroma dopolniti ter ga poslati v potrditev vodstvu.

Če so potrebne spremembe ali dopolnitve zaradi uskladitve Krovne politike in pripadajoče dokumentacije s področno zakonodajo, internimi pravilniki in zahtevam ISO/IEC 27001 standarda, Skrbnik informacijske varnosti vloži predlog za spremembo in dopolnitev z obrazložitvijo, ki ga obravnava Varnostni forum.

V primeru, da je predlog za spremembo ali dopolnitev zavrnjen, se lahko predlog ponovno vloži v roku 6 mesecev od dneva zavrnitvenega odgovora na prvotni predlog.

6 PRAVNA PODLAGA

Pri uvajanju in izvajanju Krovne politike, elementarnih varnostnih politik, pravilnikov, navodil, izjav in postopkov informacijske varnosti se upošteva veljavna zakonodaja Republike Slovenije, standard ISO/IEC 27001:2013 in dobre prakse na področju varovanja informacij.

7 OBRAVNAVANJE KRŠITEV KROVNE POLITIKE IN NAČRT UKREPANJA

Vsak uporabnik je dolžan varovati informacije, informacijska sredstva in druge vire informacij, s katerimi se seznani pri opravljanju obveznosti iz delovnega razmerja, ki jih ne sme razkriti izven okolja UL.

Vsi uporabniki lahko po anonimni poti prijavijo varnostne incidente Skrbniku informacijske varnosti. Slednji je dolžan incident dokumentirati in ustrezno ukrepati, skladno z Operativnimi navodili za upravljanje z varnostnimi incidenti.

Vsako obvestilo o sumu kršitve Krovne politike in/ali Politike informacijske varnosti se obravnava posebej. V času preiskave se lahko odvzamejo dodeljene pristopne pravice, pristojnosti oziroma pooblastila. Vsak poskus izogibanja postavljenim varnostnim kontrolam za dostop do sredstev, nagovarjanje k temu dejanju, neprimerna ali zlonamerna uporaba sredstev, se šteje za kršitev politike.

Kršitev politike pomeni ogrožanje premoženja UL in se zato obravnavajo enako, kot nevestno opravljanje dela ali drugačno namerno ali nenamerno povzročanje škode UL. Vsaka kršitev se obravnava formalno in se lahko izrečejo nedisciplinski ukrepi za lažje kršitve. Kršitev politik se obravnava po veljavni zakonodaji in pogodbi o zaposlitvi. V primeru kršitev varnostnih politik se ukrepa skladno z zakonodajo in predpisanimi pravili, opredeljenih v politikah. Proti zunanjim izvajalcem se ukrepa skladno s podpisano pogodbo, ki vključuje zahtevo po varovanju poslovne skrivnosti in osebnih podatkov.

8 REFERENČNI DOKUMENTI

1) SIST ISO/IEC 27000:2018 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Pregled in izrazoslovje.
2) SIST ISO/IEC 27001:2013 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve.
3) SIST ISO/IEC 27002:2013 Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri kontrolah informacijske varnosti.