Uprava
UL 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

POLITIKE INFORMACIJSKE VARNOSTI UNIVERZE V LJUBLJANI

Datum:
Avtor: Rektorat Univerze v Ljubljani
Verzija: 1.0
Klasifikacija: interno

OSNOVNI PODATKI O DOKUMENTU

Organizacija	Univerza v Ljubljani
Naslov	Politike informacijske varnosti Univerze v Ljubljani
Avtor	Rektorat Univerze v Ljubljani
Skrbnik dokumenta	Skrbnik informacijske varnosti
Odgovorni za izvajanje	Skrbnik informacijske varnosti
Področje	Informacijska varnost
Klasifikacija	Interno
Datum sprejetja	

ZGODOVINA RAZLIČIC DOKUMENTA

Datum	Verzija	Oseba	Kratek opis
	1.0	Skrbnik informacijske varnosti	Vzpostavitev dokumenta

KAZALO

UVOD

Politike informacijske varnosti Univerze v Ljubljani (v nadaljevanju Politike informacijske varnosti) so sprejete na podlagi poglavja 5 Struktura dokumentacije varnostne politike Krovne politike informacijske varnosti na UL (v nadaljevanju Krovna politika). Ta dokument se uporablja za uporabnike rektorata, članic UL (v nadaljevanju pristopnice UL) in pridruženih članic UL, ki so Politike informacijske varnosti, katere predstavljajo enotne zahteve in priporočila uporabnikom, uvrstile med interne akte z namenom sistematičnega izvajanja sistema upravljanja varovanja informacij (v nadaljevanju SUVI) na celotni UL. Pristopnica UL in pridružena članica UL ima možnost na podlagi poglavja 5 Struktura dokumentacije varnostne politike Krovne politike sprejeti svoje Politike informacijske varnosti in drugo pripadajočo dokumentacijo, ki mora biti skladna z zahtevami in priporočili področne zakonodaje, standarda ISO/IEC 27001:2013 in temi politikami.

S tem dokumentom vodstvo UL vzpostavlja Politike informacijske varnosti, ki zagotavlja, da UL učinkovito in uspešno vodi, nadzoruje in varuje informacijska sredstva, ki so v lasti ali najemu UL kot tudi podatke drugih pravnih in fizičnih oseb, s katerimi razpolaga.

Politika informacijske varnosti je uvrščena v klasifikacijski razred interno in je objavljena na intranetnih straneh UL ter ni namenjena širši javnosti.

Politika informacijske varnosti je sprejeta dne _____.

Politika informacijske varnosti začne veljati naslednji dan po objavi na intranetni strani UL.

1 SLOVAR IZRAZOV

Izrazi, ki se nanašajo na SUVI, so prvotno definirani v ISO/IEC 27000:2018. V tem dokumentu uporabljeni izrazi imajo naslednji pomen:

Delovna postaja je namizni ali prenosni osebni računalnik, ki je v lasti ali najemu UL in je dan uporabniku v uporabo za izvajanje obveznosti iz delovnega ali drugega pogodbenega razmerja z UL.

Dogodek je ugotovljen pojav v stanju sistema, storitve ali omrežju, ki kaže na morebitno kršitev SUVI ali okvaro zaščit, ali predhodno neznana situacija, ki je lahko pomembna za SUVI. Dogodek je lahko en ali več dogodkov in ima lahko tudi več vzrokov. Vsak dogodek je zabeležen, še posebej tisti, ki predstavlja tveganje ali grožnjo SUVI.

Grožnja je specifičen dogodek ali aktivnost, ki lahko povzroči škodo UL z izkoriščanjem ranljivosti informacijskih sredstev.

Incident je en ali več neželenih ali nepričakovanih dogodkov, ki imajo negativni učinek na SUVI, za katerega je velika verjetnost, da bodo ogrozili poslovanje in varovanje informacij na UL.

Informacije so sredstva, ki so, tako kot druga pomembna poslovna sredstva, bistvena za poslovanje UL, zato jih je treba ustrezno varovati. 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. Informacije se lahko prenašajo preko kurirja, z elektronsko ali verbalno komunikacijo.

Informacijsko okolje UL se sestoji iz programske in strojne opreme; strojna oprema vključuje strežnike, aktivno in pasivno omrežno opremo, delovne postaje s pripadajočimi perifernimi napravami, tiskalnike

in fotokopirne naprave, enote za varnostno kopiranje, prenosne nosilce podatkov in drugo strojno opremo, ki je v lasti ali najemu UL, ki so namenjeni zbiranju, obdelavi, shranjevanju in posredovanju informacij (v nadaljevanju se uporablja enoten izraz informacijski sistem).

Informacijsko omrežje UL Metulj je razdeljen na hrbtenični del za katerega skrbi USI in na LAN del, ki je za požarno pregrado na pristopnicah UL in pridruženih članicah UL. Informacijsko okolje za požarnimi pregradami je v pristojnosti pristopnic in pridruženih članic UL.

Informacijsko omrežje pristopnic UL za požarnimi pregradami so v pristojnosti pristopnic UL.

Informacijska sredstva so zlasti delovne postaje, tablice, mobilni telefoni, prenosni diski, podatkovne zbirke, datoteke z informacijami, sistemska dokumentacija, operativni in podporni postopki, uporabniški priročniki in navodila ipd., ki so v lasti ali najemu UL. V nadaljnjem besedilu se smiselno uporablja informacijska sredstva.

Informacijska varnost je zaščita, varovanje in obramba omrežja UL z zagotavljanjem zaupnosti, avtentičnosti, celovitosti in razpoložljivosti informacij, kar vključuje uporabo in upravljanje ustreznih kontrol, ki vključujejo upoštevanje groženj z namenom zagotavljanja trajnega poslovnega uspeha in kontinuitete ter zmanjševanje posledic incidentov informacijske varnosti.

Informacijski viri so vsa fizična sredstva, storitve, programska oprema in informacije, zapisane v kakršni koli obliki, ki omogočajo doseganje poslovnih ciljev s pomočjo informacijske tehnologije. V nadaljnjem besedilu se smiselno uporablja informacijska sredstva.

Krovna politika je skrajšano za Krovno politiko informacijske varnosti na UL.

Nosilec podatkov so vse vrste sredstev, na katerih so zapisani ali posneti podatki (listine, akti, gradiva, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniškimi mediji, fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov ipd.).

Podatek je neko dejstvo o določeni stvari, s katerim opredelimo informacijo.

Pridružene članice UL so po Statutu UL visokošolski in raziskovalni zavodi ali druge pravne osebe, ki dopolnjujejo dejavnost UL in dvigujejo njen ugled. V času sprejema tega dokumenta so: IRI, NUK in CTK.

Pristopnice UL se smiselno uporablja za vse tiste članice UL, ki so ta dokument sprejele, uvrstile v svoje interne akte in ga izvajajo z namenom sistematičnega izvajanja SUVI na celotni UL (akademije in fakultete).

Programska oprema je zbirka programov, s katerimi obdelujemo podatke z računalnikom. Lahko je uporabniške ali sistemske narave.

Pogodbeni izvajalec je fizična ali pravna oseba, ki ima sklenjeno pogodbeno razmerje z UL o opravljanju neke storitve ali dobavo nekega blaga v zameno za dogovorjeno plačilo.

Ranljivost je slabost vira. Gre za njegovo naravno lastnost.

Sistem upravljanja varovanja informacij (SUVI) je dokumentiran organizacijski sistem za upravljanje človeških in drugih virov s ciljem varovanja informacij in podatkov; ima postavljeno politiko, opredeljene postopke z odgovornostjo.

Skrbnik informacije (smiselno za to politiko) je pooblaščeni uporabnik informacije oziroma informacijskega sredstva, ki je odgovoren za celovitost, razpoložljivost in zaupnost informacije ter sprejema odločitve o dostopu oziroma prenosu informacije uporabnikom ali tretjim osebam.

Služba za informatiko ali služba za pomoč uporabnikom je lahko lastna ali najeta pri zunanjem pogodbenem izvajalcu.

Sredstva programske opreme so aplikacijska programska oprema, temeljna programska oprema in razvojna orodja ter podporni programi.

Tretje osebe so osebe, ki ne spadajo v kategorijo uporabnika, zaposlenega, pogodbenega izvajalca ali študenta.

Tveganje je možnost, da se pripeti nekaj nezaželenega, slabega, nesreča, izguba ali katero koli drugo nepredvideno stanje, ki predstavlja grožnjo, s katero se lahko izkoristi ranljivost informacijskih sredstev UL, in lahko posledično povzroči incident.

UL je kratica za Univerzo v Ljubljani, ki je po Statutu UL pravna oseba in v pravnem prometu nastopa v svojem imenu in za svoj račun. Če ni drugače določeno, se kratica uporablja za vse organizacijske enote rektorata UL, pristopnice UL ter njihove organizacijske enote in pridružene članice UL.

Uporabnik je oseba, ki za namene opravljanja obveznosti iz delovnega ali drugega pravnega razmerja uporablja informacijska sredstva, ki so v lasti ali najemu UL. Ta izraz se uporablja enotno za vse zaposlene, pogodbene izvajalce, študente in tretje osebe.

Vodstvo so osebe, ki usmerja in nadzoruje UL na najvišji ravni z dajanjem ustreznih pooblastil in zagotavljanjem virov za uspešno in učinkovito delovanje UL.

Zaposleni so osebe, ki imajo sklenjeno delovno ali drugo pogodbeno razmerje z UL in za namene opravljanja obveznosti iz delovnega razmerja uporabljajo informacijska sredstva, ki so v lasti ali najemu UL.

Zasebna informacijsko-komunikacijska sredstva so zlasti prenosne delovne postaje, tablice, pametni telefoni, prenosni mediji in druga zasebna sredstva, priključena v informacijsko omrežje UL.

2 PODROČJE UPORABE

Politike informacijske varnosti se dosledno upoštevajo, uporabljajo in izvajajo pri vsakodnevnem delu uporabnikov oziroma vseh tistih oseb, ki imajo omogočen dostop do informacij oziroma informacijskih sredstev, ki so v lasti in/ali v najemu UL, na način, da se zagotovi visoka raven varnosti omrežja, informacijskih sistemov, informacijskih sredstev in drugih informacij, ki so bistvenega pomena za nemoteno delovanje in poslovanje UL. V SUVI so vključeni vsa informacijska, človeška, fizična in organizacijska sredstva UL.

Obdelava osebnih podatkov se izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov.

2.1 Predmet zaščite

Politike informacijske varnosti se nanašajo na informacijska sredstva UL, med katerimi izpostavlja najpomembnejše:

- osebni podatki o zaposlenih in študentih UL,

- poslovne informacije UL,
- poslovne informacije pogodbenih izvajalcev UL,
- vse ostale informacije, ki jih je treba varovati na podlagi zakonskih in drugih predpisov oziroma drugih pravnih razmerij.

Osnovna lastnost SUVI je stalen razvoj, izboljševanje učinkovitosti in uspešnosti ter izobraževanje zaposlenih v povezavi z varovanjem informacij.

Vsak poskus obhajanja varnostnih in administrativnih kontrol dostopov do informacij oziroma informacijskih sredstev se šteje za hujšo kršitev Politike informacijske varnosti in se ukrepa skladno s poglavjem 7 Obravnavanje kršitev Krovne politike in načrt ukrepanja.

3 NAČELA VAROVANJA INFORMACIJ

Načelo celovitosti pomeni, da skrbnik informacije skrbi za popolnost in pravilnost določene informacije.

Načelo odgovornosti pomeni, da je vsak uporabnik dolžan pri delu z informacijskimi sredstvi, ki so v lasti UL ravnati z največjo mero skrbnosti, na način, da zagotovi celovitost, razpoložljivost in zaupnost informacij, ki jih pri izpolnjevanju obveznosti iz delovnega razmerja obdeluje.

Načelo poštenosti pomeni, da mora vsak uporabnik v skladu s svojimi pooblastili dosledno in pošteno obdelovati informacije, ki so v lasti UL.

Načelo sorazmernosti pomeni, da vsak uporabnik lahko dostopa zgolj do takšnega obsega informacij, kakršnega potrebuje za izpolnjevanje obveznosti iz delovnega razmerja.

Načelo zaupnosti pomeni, da je informacija dostopna le pooblaščenim osebam, ki jo varujejo pred njenim razkritjem in drugo obdelavo.

Načelo razpoložljivost pomeni, da je informacija dostopna v trenutku, ko jo uporabnik potrebuje z vnaprej znanim in zakonitim namenom uporabe.

4 SKRBNIŠTVO NAD INFORMACIJAMI IN INFORMACIJSKIMI SREDSTVI

Skrbnik informacij je odgovoren za ustrezno upravljanje z informacijami in informacijskimi sredstvi. Skrbnik informacij skrbi za zaupnost, celovitost in razpoložljivost informacij in informacijskih sredstev, odobri primeren dostop do njih ter ustrezno označevanje in upoštevanje klasifikacijske kategorije. Skrbnika informacije oziroma informacijskega sredstva določi njegov nadrejeni ali vodstvo.

Ob vsakem sumu neskladja z načeli varovanja informacij je skrbnik informacije dolžan poskrbeti, da se informacije in informacijska sredstva ne bodo razkrila, izbrisala ali kakor koli drugače poškodovala ter bodo nadzorovana znotraj omrežja UL oziroma pristopnic UL. V primeru potrjenega suma neskladja, je skrbnik informacije dolžan o tem obvestiti skrbnika informacije varnosti, ki bo v sklopu svojih pristojnosti ustrezno ukrepal.

4.1 Uporabniki informacij

Vsak uporabnik, ki ima pravico do uporabe informacij in informacijskih sredstev, ki so v lasti in/ali najemu UL in je odgovoren za ustrezno varovanje. Uporabnik mora upoštevati postavljene varnostne mehanizme in kontrole, določene s Politikami informacijske varnosti in drugimi internimi akti, ki določajo

pravice in obveznosti uporabnikov pri delu z informacijskimi sredstvi. Uporabniki informacij lahko dostopajo, uporabijo in obdelujejo informacije skladno z danimi pooblastili, ki določajo pravice za dostop. V primeru pridobitve dostopa do informacije, za katerega uporabnik nima danega pooblastila, mora o tem nemudoma obvestiti skrbnika informacije oziroma osebo, ki je dostop omogočila.

5 KLASIFIKACIJA INFORMACIJ

Informacija mora biti ustrezno klasificirana v skladu s presojo zaupnosti informacije, ki jo uvrsti v naštete kategorije, skrbnik informacije. Ravni oziroma kategorije za klasifikacijo informacij so naslednje:

- ZAUPNO pomeni, da ima razkritje pomemben kratkoročni vpliv na delovanje UL ali strateške cilje, kot so npr. strateški načrti, osebni podatki, finančni podatki, podatki zunanjih izvajalcev. Tako klasificirana informacija mora biti ves čas nadzorovana.
- INTERNO pomeni, da razkritje povzroči manjšo zadrego ali manjšo težavo pri delovanju in poslovanju UL, kot so npr. operativni podatki, zunanje pogodbe s partnerji.
- JAVNO pomeni, da razkritje ne povzroči škode UL.

V odvisnosti od stopnje zaupnosti morajo biti vse informacije ustrezno označene, upravljane, shranjene in uničene. Vsaka informacija UL, ki ni posebno klasificirana in označena, se smatra kot »INTERNO«. V uporabi so še druge kategorije klasifikacije informacij, ki se obravnavajo v skladu s predpisi, ki urejajo področje tajnih podatkov in poslovno skrivnost. Informacije, ki jih skrbnik informacije kategorizira kot JAVNO se posebej ne označuje.

6 OBVLADOVANJE TVEGANJ

Obvladovanje tveganj je urejeno generalno za celotno UL, ki vključuje tudi informacijsko varnost. Dokument, ki prepoznava tveganja za celotno UL, je dostopen tukaj (<povezava>).

POLITIKA RABE, VAROVANJA IN UPRAVLJANJA INFORMACIJSKIH SREDSTEV

1 POOBLASTILA IN ODGOVORNOSTI

Postavitev politike	Varnostni forum
Izvajanje	**Vsi redno in pogodbeno zaposleni** na UL ter drugi, ki delajo na UL. **Kadrovska služba,** za začetek postopka dodeljevanja pristopnih pravic v okviru postopkov pri sprejemu novega delavca v delovno razmerje, pri zamenjavi delovnega mesta znotraj UL in pri zaključku delovnega razmerja. **Vodje organizacijskih enot** so pristojni in odgovorni za odobritev naloga za dodelitev pravic za neposredno podrejene in za zunanje uporabnike za sisteme, katerih skrbniki so. **Pooblaščeni skrbnik informacijskega sistema** izvaja postopek dodeljevanja pravic v skladu s to politiko in vodi evidenco pristopnih pravic za uporabnike informacijskega sistema za katerega je določen kot skrbnik.
Nadzor nad izvajanjem politike	Skrbnik informacijske varnosti
Komu je namenjena	Vsem redno in pogodbeno zaposlenim, zunanjim izvajalcem, skrbnikom informacijskih sistemov ter drugim, ki na kakršnikoli način dostopajo do informacij, podatkov na informacijskih sistemih, ki so v lasti ali najemu UL ali dodeljujejo oziroma odobravajo dostop do teh sistemov.

2 NAČELA PRI RABI, VAROVANJU IN DODELJEVANJU PRAVIC DOSTOPA DO INFORMACIJ

Vsak poskus, pomoč ali nagovarjanje drugega k obhajanju varnostnih in administrativnih kontrol dostopov do informacijskih sredstev ali kršitev te politike se šteje za kršitev te politike in se obravnava skladno s Krovno politiko.

Uporabniki so dolžni o sumu kršitev ali kršitvi te politike v najkrajšem možnem času poročati skrbniku informacijske varnosti ali nadrejenemu, ta pa je dolžan to sporočiti skrbniku informacijske varnosti.

Osebni podatki, ki se obdelujejo v informacijskem okolju UL, se obdelujejo skladno s predpisi, ki urejajo področje varstva osebnih podatkov.

Zaposlenim se omogoči dostop le do informacij, ki jih potrebuje za opravljanje obveznosti iz delovnega razmerja in so razvrščene v razred »Interno«, tako, da se upošteva načelo sorazmernosti.

Zahtevek za dostop do informacije poda s strani posameznika neposredno nadrejena oseba, ki utemeljeno potrebuje dostop, katerega ga odobri Skrbnik informacije. Dodelitev pravice do informacije praviloma izvede Služba za informatiko na podlagi odobrenega zahtevka.

2.1 Načela za ločevanje nalog in pooblastil administratorjev

Skrbniki sistemov UL nastopajo tudi v vlogi administratorja sistema in imajo natančno določene pristojnosti z danim pooblastilom. Razdelitev ustreznih pooblastil je nujno potrebna z namenom preventivne preprečitve prevelike koncentracije pooblastil in pristojnosti samo eni osebi. Izjemoma lahko vodstvo dodeli pooblastila administratorja eni osebi. Za posebne sisteme, kjer so pogoji delovanja definirani z zakonom oziroma podrejenimi akti, se način dela in dodeljevanje pooblastil administratorjem podrejajo tem aktom.

V primeru odsotnosti prvotnega administratorja lahko na podlagi posebnega pooblastila nadomesti t.i. nadomestni administrator, ki ga pooblasti prvotni administrator za vnaprej določeno aktivnost.

Vsak poseg v operacijski sistem, podatkovno bazo, aplikacijo ali nastavitev pravic uporabnika se beleži v dnevniku dostopov, ki se lahko nahaja v elektronski ali fizični obliki.

3 UPRAVLJANJE INFORMACIJSKIH SREDSTEV

3.1 Popis sredstev

Vsa informacijska sredstva so redno spremljana, upravljana in popisana. Vsaj enkrat letno oziroma ob vsaki spremembi opravi vsakokrat imenovana inventurna komisija popis vseh informacijskih sredstev in po potrebi določi skrbništvo oziroma odgovorne osebe za sredstva, ki jih lahko uporablja več ljudi. Evidenca popisa se hrani v elektronski obliki.

3.2 Primerna raba sredstev UL

Vsa informacijska sredstva UL se prvovrstno uporabljajo le v službene namene. Ne glede na to se informacijska sredstva lahko uporabljajo v omejenem obsegu in razumnih mejah tudi v zasebne namene, vendar ne smejo posredno in neposredno ogrožati varnosti UL in kršiti to politiko. Delovne postaje se izven delovnega mesta ne sme puščati izven nadzora ali dajati v uporabo tretjim osebam brez vednosti zaposlenega.

Zaposleni morajo delovne postaje ob izhodih iz pisarne in ob koncu delovnega dne zaradi preprečitve dostopa nepooblaščenih oseb zakleniti (politika čistega zaslona) oziroma ugasniti. Praviloma Služba za informatiko nastavi na delovnih postajah samodejno zaklepanje zaslona po 10 minutah neaktivnosti. Vstop v delovno postajo po zaklepanju je možen samo z vnosom gesla.

Zaposleni na svojih delovnih postajah ne smejo imeti administratorskih pravic. Administratorske pravice imajo na svojih delovnih postajah le skrbniki informacijskega sistema UL in/ali vodstvo. Izjemoma se lahko na predlog vodstva posameznim uporabnikom zaradi obveznosti iz delovnega razmerja dodelijo oziroma odvzamejo pravice lokalnega administratorja delovne postaje, ki tem uporabnikom omogočajo namestitev dodatne programske opreme na delovnih postajah, ki jih uporabljajo. Na informacijska sredstva UL sme Služba za informatiko nameščati licenčno programsko opremo. Uporabnik ne sme nameščati programske opreme brez vednosti Službe za informatiko. Uporabnik lahko sam namesti programsko opremo samo iz virov proizvajalca programske opreme. Za takšno namestitev je odgovoren uporabnik sam. V primeru dvomov se mora uporabnik posvetovati s Službo za informatiko.

Ta pravila veljajo tudi za rabo informacijskih sredstev izven prostorov UL.

3.2.1 Pravila za gesla

Uporabnik mora gesla hraniti kot zaupno informacijo in jih ne sme deliti z nikomer. Gesla so lahko zapisana na elektronskih medijih, ki so dodatno varovani - enkripcijo in so skladna z veljavnimi operativnimi navodili. Uporabniku je prepovedano uporabljati osebno geslo druge osebe.

Zahteve za upravljanje gesel (kompleksnost, perioda menjave in druge omejitve) opredeljujejo operativna navodila.

3.2.2 Prenosni telefoni

Uporabniku, ki je dana v uporabo mobilna naprava, ki je v lasti ali najemu UL, mora poskrbeti za njeno ustrezno varnost, tj. avtomatično zaklepanje telefona s kodo, geslom ali prstnim odtisom po nekaj minutni neaktivnosti, s PIN kodo ali geslom varovana SIM kartica. Sprejemljiva uporaba mobilne naprave je določena s Pravilnikom o uporabi službenih mobilnih naprav. Mobilna naprava mora imeti nameščeno zadnjo različico operacijskega sistema in nameščenih aplikacij. Mobilna naprava se lahko poveže le na predhodno preverjeno in zaupanja vredno brezžično omrežje. Pri posredovanju informacij preko mobilne naprave se upošteva načelo zaupnosti in po potrebi uporaba kriptografske metode.

3.2.2.1 Zamenjava uporabnika

Služba za informatiko, če ni drugače dogovorjeno, opravi začetno inicializacijo mobilne naprave (ang. factory reset), tako, da se izbrišejo vse informacije in po potrebi zamenja spominsko kartico.

3.2.2.2 Popravila, uničenje, odprodaja

Popravila mobilnih naprav lahko izvaja le od UL pooblaščeni servis z ustrezno podpisano izjavo o varovanju poslovnih skrivnosti in osebnih podatkov. Če obstajajo tehtni razlogi, da mora popravilo izvesti tretji servis, tj. servis, katerega UL ni pooblastila, mora uporabnik to predhodno uskladiti s Službo za informatiko. Preden se naprava odproda ali posreduje pogodbenemu izvajalcu v uničenje, mora Služba za informatiko izbrisati vse informacije, tako, da je onemogočena njihova obnovitev.

3.2.3 Tiskalniki

Zaposleni UL, ki pri izvajanju svojih delovnih obveznosti kopirajo, na drug tehnični način razmnožujejo ali tiskajo dokumente, ki vsebujejo informacije, pomembne za UL, na napravah, ki jih uporablja večje število zaposlenih, po končanem kopiranju ali tiskanju ne smejo puščati dokumentov v, na ali ob teh napravah. Tiskalniki naj omogočajo preverjanje osebne prisotnosti, bodisi z identifikacijsko kartico, če tiskalnik to omogoča. Tiskalnik, ki omogoča takšen način tiskanja, naj bo omogočena samodejna odjava po neaktivnosti.

3.2.4 Faks z zaupnimi informacijami

Zaupne informacije lahko uporabnik pošilja po faksu le, če je to nujno potrebno in v danem trenutku ni druge možnosti. Zaupne informacije se pošiljajo vnaprej preverjenemu prejemniku z označbo ZAUPNO. Za varno pošiljanje zaupne informacije je odgovoren pošiljatelj.

3.2.5 Internet

Internet se uporablja v službene namene. Ne glede na to se informacijska sredstva lahko uporabljajo v omejenem obsegu in razumnih mejah tudi v zasebne namene, vendar ne smejo posredno ali neposredno ogrožati varnosti UL in kršiti to politiko. Internetne strani, ki se pregledujejo v zasebne namene, ne smejo vsebovati neprimerne ali žaljive vsebine. Vodstvo UL lahko s posebno odredbo odredi blokado določenih spletnih strani. Blokado dostopa do določenih spletnih strani izvede skrbnik informacijskega sistema, na podlagi pisne odredbe vodstva. O blokadi obvestijo vse zaposlene po elektronski pošti. Blokada velja do preklica.

Redno se spremljajo poskusi vdorov v omrežja UL in sprejemajo ukrepi za odpravo tveganj. Vzpostavljena je zaščita pred vdori iz interneta s sistemom požarnih pregrad z demilitarizirano pol varno cono (DMZ) s strežniki, ki so dostopni iz interneta in notranjega omrežja. Skrbniki informacijskih sistemov, ki so v DMZ in drugih mrežnih območjih, morajo skrbeti za redno posodabljanje strežnikov oziroma če to ni mogoče, drugače zmanjšati ter omejiti tveganje za vdor. O tem se vodi evidenca. Za potrebe zagotavljanja napredne varnosti ter analize varnostnih dogodkov in incidentov ali diagnostike težav se lahko na jedrni IT infrastrukturi izvajajo napredne metode spremljanja mrežnega prometa (npr. DPI, detekcija in avtorizacija uporabnikov ipd.).

3.2.6 Elektronska pošta

Elektronska pošta se uporablja v službene namene. Ne glede na to se lahko e-pošta uporablja v omejenem obsegu in razumnih mejah tudi v zasebne namene, vendar ne sme posredno ali neposredno ogrožati varnosti UL in kršiti to politiko, upoštevaje poglavja 3.2.7.1 Nedovoljena uporaba. E-pošte je varovana in zaščitena z geslom.

E-pošta uporabnikov je varovana pred nepooblaščenim dostopom, spremembo ali zavrnitvijo storitve, zagotavljanje pravilnega naslavljanja in prenosa sporočila, zanesljivost in razpoložljivost storitve, omogočeno je pošiljanje e-pošte z elektronskim podpisom in druge smiselne kontrole.

Zaupne informacije se pošiljajo vnaprej preverjenemu prejemniku v šifrirani obliki z označbo zaupna občutljivost in visoka pomembnost. Za varno pošiljanje zaupne informacije je odgovoren pošiljatelj. Podrobneje je urejeno z operativnimi navodili.

Če se pojavi utemeljen sum, da uporabniki ne spoštujejo omejitev iz poglavja 3.2.7.1 Nedovoljena uporaba, lahko skrbnik informacijskega sistema na posebej utemeljeno pisno zahtevo vodstva opravi nadzor prometnih podatkov in količine uporabe e-pošte, a zgolj z vidika odkrivanja vzrokov za prekomerno obremenjevanje strežnika. Pri tem se ne sme pregledovati vsebine e-pošte. Vpogled in dostop se opravi skladno z operativnimi navodili.

Aktivno se izvaja se nadzor e-pošte v smislu odkrivanja neželenih vsebin z orodji za prepoznavanje.

V sistemu e-pošte UL spoštuje pravico do zasebnosti, sorazmerno z zakonitim ciljem, ki mu UL sledi in ne izvaja nadzora nad vsebino e-pošte, razen kadar pride do kolizije z drugimi ustavnimi pravicami, ki lahko prevladajo.

3.2.6.1 Nedovoljena uporaba

E-pošta UL se ne sme uporabljati za kreiranje in razpošiljanje kakršnih koli motečih ali žaljivih sporočil, ki vsebujejo žaljive komentarje glede rasne ali nacionalne pripadnosti, spola, barve kože, las ali oči, starosti, spolne usmerjenosti, verskega ali političnega prepričanja, ali imajo pornografsko vsebino. V primeru prejema takšnega sporočila, mora uporabnik nemudoma podati prijavo skrbniku informacijske varnost ali skrbniku informacijskega sistema ali nadrejenemu.

Izrecno prepovedano je:

- množično pošiljanje e-pošte brez pooblastila ali na način, ki lahko ogroža varnost UL,
- ustvarjanje in razširjanje zlonamernih informacij,
- pošiljanje neprimernih vsebin iz e-poštnega sistema UL,
- zavestno pošiljanje zlonamerne kode, brez vnaprej danega pisnega dovoljenja vodstva UL,
- nepooblaščeno pošiljanje sporočil z obvestili o zlonamerni programski kodi,
- pošiljanje verižnih pisem,
- poplavljanje z e-pošto,
- prenašanje programov, glasbe in videa, pri katerih se kršijo avtorske pravice,

- uporaba e-pošte UL za zasebno nakupovanje na spletu.

3.2.6.2 Avtomatsko posredovanje elektronske pošte

Prepovedano je avtomatsko posredovanje e-pošte zunanjim prejemnikom, kar vključuje tudi zaseben ali drug poštni predal izven UL, razen kadar je to pomembno za poslovanje UL, pri čemer pa je treba poskrbeti za zaupnost tako posredovane pošte.

3.2.7 Digitalna identiteta

Vsakemu uporabniku se na podlagi zahtevka, ki ga posreduje kadrovska služba, dodeli unikatno uporabniško ime, ki ga lahko uporablja samo njegov lastnik. Posojanje uporabniškega imena ni dovoljeno. Prav tako ni dovoljena uporaba skupinskih uporabniških imen. Uporaba digitalne identitete je namenjena le službeni rabi. Pojem digitalna identiteta zajema vse digitalne identifikacijske načine, ki se uporabljajo za digitalno komunikacijo in so vezani na UL ali so bili dodeljeni s strani UL oziroma so bili odprti za opravljanje obveznosti iz delovnega razmerja.

3.2.8 Uporaba zasebnih informacijsko-komunikacijskih sredstev (BYOD)

Uporaba zasebnih informacijsko-komunikacijskih sredstev v informacijskem omrežju UL je dovoljena le, če je to potrebno zaradi opravljanja delovnih obveznosti in na podlagi predhodnega pisnega dovoljenja vodstva. Zasebna informacijsko-komunikacijska sredstva morajo biti pred uporabo in med uporabo preverjena glede prisotnosti virusov, škodljive ter nezaželene programske kode in vsebine. Uporabniki morajo osebam, odgovornim za delovanje informacijskega okolja UL izkazati prisotnost ustreznih varnostnih kontrol na svoji napravi (posodobljena protivirusna zaščita, ipd.). V primeru sporov glede uporabe takšnih sredstev v informacijskem okolju so odgovorne osebe dolžne obvestiti skrbnika informacijske varnosti.

Namestitev programske opreme za dostop do informacijskega okolja UL in dodelitev, sprememba ali odvzem pripadajočih uporabniških pravic na zasebna informacijsko-komunikacijska sredstva je možna samo na podlagi predhodnega pisnega dovoljenja vodstva. Zasebnih informacijsko-komunikacijskih sredstev se ne sme vključevati v domeno UL.

3.3 Varnostno kopiranje informacij na delovnih postajah

Za varnostno kopiranje informacij na delovnih postajah je odgovoren vsak zaposleni. Informacije lahko shranjuje le na dopustnih mestih in na način, ki je predviden v operativnih navodilih. Za morebitno okvaro ali izgubo informacij, ki izvirajo iz delovnih obveznosti na drugih mestih, odgovarja zaposleni sam. Služba za informatiko zagotavlja pomoč pri varnostnem kopiranju. O varnostnem shranjevanju se vodi evidenca. Postopek in obseg varnostnega shranjevanja je natančneje opredeljen v operativnih navodilih.

3.4 Izvajanje politike čiste mize in praznega zaslona

Z namenom varovanja informacijskih sredstev je treba vse nosilce podatkov in dostope do informacij ustrezno varovati, skladno s sprejetimi internim aktom, ki ureja politiko čiste mize in praznega zaslona.

3.5 Primerna raba strojna oprema

Vsa strojna oprema se uporablja s svojo namembnostjo in v službene namene. Uporablja in vzdržuje se v skladu z navodili proizvajalca in politikami.

3.6 Priključevanje opreme v omrežje

Vsaka priključena (brezžična) oprema mora imeti vgrajene najnovejše varnostne mehanizme: popravki operacijskega sistema, požarno pregrado, po potrebi redno ažurirano protivirusno zaščito ter ustrezno zaprta komunikacijska vrata. Spremembe na opremi končnih uporabnikov se lahko izvaja le v skladu z navodili Službe za informatiko.

3.7 Iznos računalniške opreme

Iz prostorov UL je dovoljen iznos le osebne prenosne računalniške opreme, kot so prenosna delovna postaja, prenosne naprave, mobilni telefoni in podobno, ob predhodnem soglasju nadrejenega. Pri presoji iznosa je treba upoštevati s tem povezana tveganja.

3.8 Uničenje in odpis informacijskih sredstev

V primeru, da je treba določeno informacijsko sredstvo ali opremo zaradi izrabljenosti, okvare, tehnološkega zastaranja ali iz drugih utemeljenih razlogov odpisati oziroma uničiti, mora Služba za informatiko v sodelovanju s komisijo, imenovano s sklepom vodstva, pripraviti predlog za uničenje ali odpis opreme ob upoštevanju internih predpisov, ki opredeljujejo ravnanje z odsluženimi sredstvi. Predlog mora odobriti vodstvo. Pred predajo v uničenje, odpis, prodajo ali podaritvijo nosilcev podatkov Služba za informatiko poskrbi, da je vsebina nosilcev podatkov nepovratno izbrisana. Uničenje informacijskega sredstva lahko opravi zunanji izvajalec, s katerim ima UL urejeno pogodbeno ali drugo pravno razmerje o sodelovanju. Priporočljivo je, da zunanji izvajalec ima veljaven certifikat ISO 14000 in podpisano izjavo o varovanju osebnih podatkov in poslovnih skrivnosti.

Za uničenje drugih informacijskih sredstev, kot je dokumentarno gradivo, se uporablja Uredba o upravnem poslovanju.

Vsak odpis in/ali uničenje mora biti ustrezno dokumentirano, na način, da se ohrani revizijska sled.

4 ROKOVANJE Z NOSILCI INFOMRACIJ/ PODATKOV

Uporabnik mora upoštevati varnostne ukrepe, ki preprečujejo nepooblaščeno razkritje, spreminjanje, odstranitev ali uničenje informacij, še posebej, če so na nosilcih podatkov zaupni podatki.

4.1 Uporaba izmenljivih nosilcev podatkov

Zaposleni, ki so jim bili dodeljeni prenosni nosilci podatkov (USB ključi, prenosni diski in ostali prenosni nosilci podatkov), so odgovorni za varnost teh nosilcev. Prenosni nosilci podatkov ne smejo vsebovati informacij prejšnjih uporabnikov tako službenih in/ali zasebnih zadev. Po uporabi prenosnih nosilcev informacij se vsebina teh nosilcev po potrebi in skladno s klasifikacijo informacije šifrira, shrani v informacijskem okolju UL, ognjevarni omari, trezorju ali nepovratno izbriše ali kakorkoli drugače varovani pred nepooblaščenim dostopom, razkritjem, spreminjanjem, odstranjevanjem ali uničenjem.

O morebitni izgubi ali kraji prenosnih nosilcev informacij mora zaposleni takoj obvestiti Službo za informatiko, ki sestavi uradni zaznamek, v katerem se navedejo okoliščine ter popiše vsebina podatkov na izgubljenih prenosnih nosilcih podatkov.

Vsaj enkrat letno skrbnik informacije pregleda vsebino, zapisano na (izmenljivih) nosilcih podatkov ter jih po potrebi varno uniči.

4.2 Šifriranje podatkov

Informacije, ki so klasificirane kot (strogo) zaupne in so na izmenljivih nosilcih informacij, ali se pošiljajo po komunikacijskih povezavah, zunaj informacijskega omrežja UL, morajo biti ustrezno šifrirani, vsaj 128 bitno z uporabo posebnih programov (npr. WinPT/Kleopatra in/ali ZIP z uporabo gesla).

5 VARNOSTNO KOPIRANJE

Varnostne kopije podatkov v informacijskem sistemu morajo biti izdelane, hranjene in preverjane skladno z zahtevami skrbnikov informacijskih sistemov. Zahteve skrbnikov morajo opredeliti podatke, ki naj jih vsebuje varnostna kopija, in pogostnost izdelave teh kopij. Postopek izdelave varnostnih kopij in njihove ponovne uporabe je podrobneje dokumentiran v operativnih navodilih.

Pravilnost delovanja samodejnih postopkov izdelave varnostnih kopij mora biti ustrezno preverjena v rednih obdobjih in pred vsako uporabo rezervnih kopij.

Pri shranjevanju varnostnih kopij na oddaljene lokacije morajo biti izpolnjeni zahtevani varnostni pogoji za prenos in shrambo varnostnih kopij.

Varnostne kopije zahtevajo enake varnostne pogoje kakor delujoča zbirka podatkov.

Dostop do varnostnih kopij mora biti primerno reguliran in spremljan. Podrobneje varnostno kopiranje in dostop do varnostnih kopij opredeljujejo operativna navodila.

6 UPRAVLJANJE SISTEMSKIH OPERACIJ

Pod pojem novi sistemi sodijo npr. nova strojna oprema, nove aplikacije, nove verzije aplikacij, nove verzije operacijskega sistema, nove baze podatkov in nove verzije baze podatkov.

6.1 Dokumentiranje postopkov

Za upravljanje sistemskih operacij se zagotavlja in vzdržuje dokumentacija za vse informacijske sisteme, v kateri so opisani postopki za namestitev, vzdrževanje, nastavitev in uporabo določene strojne ali programske opreme, pri čemer se primarno in smiselno uporablja dokumentacija proizvajalca, za potrebe končnih uporabnikov pa se ta ustrezno prilagodi, ki je evidentirana po verzijah in dostopna uporabnikom na intranetnih straneh UL. Na UL se smatra sistemska dokumentacija (načrti, sheme, konfiguracije …) kot zaupni dokument in se varuje skladno s stopnjo zaupno.

6.2 Ločeno testno in produkcijsko okolje

Na UL se za ključne informacijske sisteme in glede na ocenjena tveganja uporabljata vsaj dve ločeni in jasno razlikovalni sistemski okolji: testno, če je na razpolago in produkcijsko z namenom zavarovanja produkcijskega okolja pred neavtoriziranimi dostopi zaradi testiranja sprememb na aplikacijski in sistemski opremi, s čimer se prepreči prehod v produkcijsko okolje, v primeru nezadostno testirane spremembe. Najbolj kritični informacijski sistemi morajo biti v produkcijskem okolju fizično ločeni in osamljeni od testnega. Uporabniki morajo uporabljati različne uporabniške profile za različna okolja.

Če se pri testiranju ali razvoju uporablja podatke iz operativnega okolja, je z njimi potrebno ravnati na enak način, kot s podatki iz operativnega okolja, podatke v razvojnem in testnem okolju pa po uporabi ustrezno uničiti. Občutljivi podatki se v originalni obliki smejo uporabljati v testnem okolju le v primeru, če je zagotovljena enaka raven avtorizacije v testnem, kot je v produkcijskem okolju.

Pravila za različna okolja se uporabljajo skladno s Politiko razvoja programske opreme.

6.3 Upravljanje zmogljivosti

Skrbnik informacijskega omrežja UL v sodelovanju s skrbniki informacijskih sistemov redno spremljajo in prilagajajo informacijske sisteme na način, da se zagotavlja izboljšanje razpoložljivosti in učinkovitosti informacijskih sistemov, tam kjer je to potrebno, ob doslednem upoštevanju potreb in zahtev, ekonomičnosti investicij v nove informacijske sisteme s preprečitvijo nastanka ozkega grla. Izdela naj se načrt upravljanja zmogljivosti in morebitne nadaljnje širitve oziroma nadgradnje.

6.4 Sprejem novih sistemov

Vsaka sprememba informacijskega sistema ali uvedba novega informacijskega sistema lahko vpliva na delovanje ostalih sistemov oziroma informacijskega sistema v celoti, zato se spremembe izvedejo skladno s Politiko upravljanja sprememb.

6.5 Ranljivosti sistemov

Skrbniki informacijskih sistemov redno spremljajo morebitne ranljivosti sistema iz verodostojnih virov in sprejemajo ustrezne ukrepe za preprečitev morebitne grožnje. Ranljivosti morajo prepoznati skrbniki informacijskih sistemov, o čemer obvestijo uporabnike in so popisani v tabeli ocena tveganj. Skrbniki informacijskih sistemov v skladu s Politiko upravljanja sprememb in Operativnimi navodili nadgrajujejo sistem z vnaprej preverjenimi in ovrednotenimi popravki oziroma novo verzijo ali ustrezno spremenijo postopke uporabe.

7 ZAŠČITA INFORMACIJ

7.1 Zaščita informacij pred izgubo

Informacije morajo biti ustrezno varovane pred nepooblaščeno obdelavo tako, da skrbnik informacije odlaga na predvidene datotečne strežnike, na katerih je zagotovljena ustrezna raven varovanja in se izvaja varnostno shranjevanje informacij, kar podrobneje urejajo operativna navodila. Na datotečnih strežnikih je prepovedano odlaganje dokumentov, slik ali video posnetkov zasebne narave. V ta namen morajo zaposleni periodično, vsaj enkrat letno brisati neprimerne datoteke iz datotečnega strežnika. Služba za informatiko lahko enkrat letno pobriše neprimerno vsebino, ki ne sodi na datotečni strežnik. Velikost datotečnega strežnika uporabnika ne sme presegati kvote, ki jo letno določi UL.

7.2 Protivirusna zaščita in požarna pregrada

Služba za informatiko skrbi za vzpostavitev in delovanje protivirusne zaščite na ravni strežnikov, delovnih postaj, komunikacijske opreme, e-poštnega sistema oziroma tam, kjer je to potrebno, ki omogoča zaščito pred zlonamerno kodo. Izključitev zaščite je dopustna le z izrecnim dovoljenjem Službe za informatiko. Uporabnik ob morebitni pomoči Službe za informatiko stalno preverja delovanje in zagotavlja sprotno posodabljanje protivirusne zaščite. V primeru dvomov in težav s protivirusno zaščito ali osebno požarno pregrado se uporabnik obrne na Službo za informatiko. Računalniška oprema, ki ni v upravljanju Službe za informatiko, mora biti preverjena na prisotnost virusov pred priključitvijo na omrežje UL. Nekontinuirano oziroma nepreverjene delovne postaje se priključijo v ločen segment omrežja, če je na voljo.

V primeru okužbe delovne postaje mora zaposleni zaustaviti (ugasniti) delovno postajo ali jo takoj izključiti iz omrežja ter kontaktirati Službo za informatiko. Minimalna priporočila so naslednja:

- Uporabnik ne sme prenašati datotek iz neznanih/nedovoljenih virov-internetnih strani, družabnih omrežij ali e-pošte,
- Uporabnik naj ne odpira priponk v e-pošti, ki je neznanega, sumljivega ali nezaupljivega izvora. Priponke in e-pošto naj takoj izbriše-tudi z mest za odlaganje prenesenih datotek.

7.3 Varovanje informacijske infrastrukture

Prepovedano je kakršno koli nepooblaščeno poseganje v informacijsko infrastrukturo, to pomeni:
- spreminjanje topologije omrežja,
- samovoljna menjava ali dodajanje nove aktivne mrežne opreme, tudi Wi-Fi naprav,
- nepooblaščen dostop, poseganje v aktivno opremo (HTTP(S) dostop, SSH, Telnet….),
- nepooblaščeno povezovanje z drugimi omrežji oziroma napravami (VPN, servisi za oddaljeno povezovanje),
- Nepooblaščeno nameščanje programske opreme, ki omogoča oddaljen dostop to opreme mimo požarne pregrade (npr. TeamViewer ipd.).

Na UL se ne smejo uporabljati komunikacijske naprave (modemi, WLAN naprave), ki niso pod upravljanjem Službe za informatiko oziroma niso upravljane v skladu z zahtevami UL.

7.4 Varovanje komunikacij

7.4.1 Lokalno omrežje

Fizična raven omrežja je nadzorovana tako, da so ožičenje, pasivna in aktivna omrežna oprema, ki predstavljajo jedrno mrežno topologijo UL, fizično in logično varovani. Na lokalno omrežje, ki ni namenjeno študentom in/ali gostom, se priključi samo preverjena in testirana oprema. Vsi LAN priključki, ki niso zasedeni in dostop do njih ni drugače varovan (npr. zaklenjen prostor z nadzorom dostopa), so na aktivni opremi onemogočeni oziroma zahtevajo avtentikacijo opreme ob vključitvi (avtentikacija 802.1x).

WiFi priključki, ki omogočajo dostop do notranjega omrežja UL, so ustrezno kriptirani. Za varovanje pred nepooblaščenim spreminjanjem konfiguracij aktivne opreme se vsi posegi beležijo na centralnem dnevniku operacij.

Omrežje je ločeno na posamezne logične dele (navidezna omrežja), med katerimi so nadzorovani prehodi. Za vsak prehod so definirana pravila, ki omogočajo dostop do izbranih servisov. Na omrežju so vzpostavljeni tudi aplikativni filtri, ki onemogočajo neavtorizirano komunikacijo. Za goste je postavljeno posebno logično omrežje, ki omogoča gostom varovan dostop do interneta.

Dostop do storitev omrežja (AD, e-pošta, WEB …) imajo samo skrbniki informacijskih sistemov, ki imajo administratorske pravice.

Na lokalnem omrežju so prepoznani kritični deli omrežja, ki predstavljajo edinstveno točko odpovedi (single point of failure). V teh kritičnih delih omrežja je glede na oceno tveganj podvojen pasivni in/ali aktivni del omrežja.

8 DOSTOP DO INFORMACIJSKEGA OKOLJA

Dostop do uporabniškega profila uporabnika na operacijskem sistemu je zavarovan z ustreznim domenskim geslom. Sistem gesel mora omogočati možnost naknadnega ugotavljanja, kdaj je bil opravljen posamezen dostop do posameznega informacijskega podsistema, kdo ga je izvedel in do katerih

informacij je dostopal (revizijske sledi). Ustreznost zapisovanja revizijske sledi redno pregleduje Služba za informatiko.

Na UL uporabniki za dostop do informacijskega okolja UL uporabljajo digitalno identiteto, razen v izjemnih primerih, kjer se zaradi tehnologije dela uporabljajo skupinska uporabniška imena, kar vodstvo odobriti.

8.1 Administratorski dostopi

Uporaba administratorskih uporabniških računov je strogo omejena in se uporablja izključno za sistemske operacije, ki to zahtevajo. Skrbniki informacijskih sistemov, ki imajo administratorske pravice uporabljajo dva uporabniška računa: privilegiranega za izvajanje sistemskih operacij ter neprivilegiranega za ostalo delo. Kjer je potrebna zanesljiva identifikacija uporabnika in so sistemi podvrženi visokemu tveganju, se uporablja močna avtentikacija. Pri prijavi administratorjev na posebnih sistemih se po potrebi uporablja avtentikacija, ki zahteva istočasno prijavo dveh administratorjev.

8.1.1 Oddaljeni dostop

Na predlog nadrejenega lahko vodstvo uporabniku omogoči oddaljen dostop do službene e-pošte ali drugih informacijskih sredstev preko VPN povezave in/ali z uporabo geselnika za varni dostop. VPN dostop se po potrebi uporablja tudi za zagotavljanje varne povezave med pristopnicami UL in drugimi sodelujočimi organizacijami. Služba za informatiko lahko preuči in predlaga uporabo drugega načina oddaljenega dostopa do informacijskih sredstev UL, ki je sprejemljiv glede na oceno tveganj.

8.2 Varna prijava na sisteme

Proces varne prijave odkriva nepooblaščenemu uporabniku čim manj informacij o sistemu. Na UL se pri prijavi v informacijski sistem upošteva vsaj naslednje:

- Prijava ne identificira sistema, dokler se prijavni postopek ne izvede uspešno.
- Izpiše se opozorilo, da je dostop omogočen le pooblaščenim uporabnikom.
- Ne omogoča sporočil za pomoč med prijavnim postopkom.
- Preverja prijavne informacije šele po vnosu vseh podatkov. Če se pojavi napaka, ne pove, kateri del podatkov je napačno vnesen.
- Določeno je število dovoljenih neuspešnih prijavnih poskusov glede na privilegije uporabnika. Po presegu tega števila se sproži prekinitev do naslednje možnosti prijave.

8.3 Pregledi dostopnih pravic

Služba za informatiko vsaj enkrat letno opravi pregled dostopnih pravic uporabnikov do posameznih informacijskih sistemov in po potrebi odvzame uporabniške dostope.

8.4 Uporaba sistemskih pripomočkov

Uporaba sistemskih pripomočkov za neposreden dostop do informacijskih sistemov je tehnično omejena na pooblaščene uporabnike in je omogočena na način, da omogoča sledljivost in dokumentiranost posegov.

9 VZDRŽEVANJE STROJNE IN PROGRAMSKE OPREME

Informacijsko okolje UL (strojna in programska oprema) je nameščena, redno pregledana in vzdrževana skladno z zahtevami proizvajalca opreme. Skrbnik informacijskega okolja ob nakupu nove strojne ali

programske opreme izdela terminski plan rednih pregledov in testiranj opreme glede na zahteve proizvajalca opreme.

10 NADZOR

Na UL so vzpostavljeni mehanizmi, ki omogočajo spremljanje in evidentiranje dogodkov: privilegirane operacije, avtorizirani dostopi in neavtorizirani poskusi dostopov, sistemske napake in alarmi, aktivnosti administratorjev in operaterjev na sistemih. Dnevniki dogodkov, kamor sodijo dostopne pravice uporabnikov in administratorjev informacijskih sistemov se redno pregledujejo, nadzirajo, varno shranjujejo in hranijo v posebnem informacijskem okolju, ki onemogoča nepooblaščeno obdelavo do teh zapisov. Zapisi o delovanju sistema se morajo hraniti najmanj do pregleda, ki ga izvede skrbnik informacijskega sistema in na podlagi katerega je pripravljen nov zapis o opravljenem pregledu in ustreznosti sistema.

Sistemska ura na vseh informacijskih sistemih se redno pregleduje in sinhronizira s centralno uro na UL, le-ta pa je sinhronizirana preko Arnesa. Uskladitev sistemskih ur v odnosu do zunanjih izvajalcev poteka na podlagi predhodnega dogovora z zunanjim izvajalcem. Skrbnik informacijskega sistema je odgovoren za sinhronizacijo ur.

Komunikacijska oprema se stalno nadzira, meri promet in število napak pri prenosu podatkov. Spremlja se tip, izvor in prenos podatkov ter ob odstopanjih od predvidenih komunikacijskih povezav ustrezno alarmira. Ti podatki omogočajo analiziranje uporabe omrežja ter pravočasno ukrepanje.

POLITIKA VAROVANJA ČLOVEŠKIH VIROV

1 POOBLASTILA IN ODGOVORNOSTI

Postavitev politike	Varnostni forum
Izvajanje	Vsi zaposleni na UL in drugi pogodbeni sodelavci
Nadzor nad izvajanjem politike	Vodja kadrovske službe
Komu je namenjena	Vsem zaposlenim na UL in druge pogodbene sodelavce, ki dostopajo in uporabljajo informacijska sredstva UL.

2 VKLJUČEVANJE VARNOSTI V DELOVNE OBVEZNOSTI

Varovanje informacij je za zaposlene določeno s pogodbo o zaposlitvi, medtem ko je za osebe s sklenjenim drugim pogodbenim razmerjem (avtorska ali podjemna pogodba) pa podpišejo dogovor o sodelovanju, ki vsebuje člen o varovanju informacij, v katerem je opredeljeno, katera so tista delovna mesta, ki so s stališča informacijske varnosti bolj in katera manj izpostavljena ter posledično prinašajo za zaposlenega večje ali manjše delovne obveznosti.

3 RAVNANJE S KADROVSKIMI EVIDENCAMI

Kadrovske evidence in osebni podatki zaposlenih, katere upravlja kadrovska služba na podlagi Zakona o evidencah s področja dela so varovani z upoštevanjem predpisov, ki urejajo varstvo osebnih podatkov ob upoštevanju delovno pravne zakonodaje in internih aktov. Posebni osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se onemogočeni nepooblaščen dostop.

4 VARSTVO PRI DELU

Kadrovska služba skrbi za varstvo pri delu skladno z Zakonom o varnosti in zdravju pri delu in drugimi internimi akti.

5 SKLENITEV DELOVNEGA RAZMERJA

5.1 Zaposlitev novega sodelavca

Nadrejeni, ki sprejme novo zaposlenega sodelavca, sproži postopke za pridobitev potrebne opreme za izpolnjevanje obveznosti iz delovnega razmerja.

5.1.1 Ravnanja pred sklenitvijo delovnega razmerja

Novo zaposleni mora biti ob sklenitvi delovnega razmerja seznanjen z vsebino Krovne politike, Politike informacijske varnosti, Operativnimi navodili in drugimi obvezujočimi internimi akti.

5.1.2 Ravnanja ob spremembi delovnega mesta

Služba za informatiko v primeru potrebe po spremembi uporabniških pravic zaradi premestitve, spremembe obsega delovnih obveznosti ali iz drugih utemeljenih razlogov, na podlagi zahtevka s strani posamezniku neposredno nadrejenih oseb ali vodstva, izvede ustrezno spremembo uporabniških pravic (sprememba, odvzem, dodelitev).

5.2 Ravnanja ob prenehanju delovnega razmerja

5.2.1 Ukinitev dostopnih pravic do informacijskih sredstev

Ob prekinitvi delovnega razmerja se zaposlenemu ukinejo vse dostopne pravice do informacijskih sredstev in se ob temu ustrezno izpolni Obrazec za odvzem uporabniških pooblastil. Zaposlenemu mora biti dana možnost, da lahko pred prekinitvijo delovnega razmerja z informacijskih sredstev UL, ki so mu bila dane v uporabo, pobriše ali si skopira osebne podatke in zasebno korespondenco, ki je nastala ob uporabi službenih sredstev v izključno zasebne namene. Ob prekinitvi delovnega razmerja zaposleni in Služba za informatiko, podpišeta primopredajni zapisnik, v katerem popišeta vsa vrnjena delovna sredstva. Sestavni del primopredajnega zapisnika je tudi izjava zaposlenega, s katero ta izjavlja:

- da mu je bila dana možnost zavarovanja lastnih osebnih podatkov in zasebne korespondence, ki je nastala ob uporabi službenih sredstev v izključno zasebne namene;
- da delovna sredstva, ki jih vrača delodajalcu, ne vsebujejo njegovih osebnih podatkov ali osebne korespondence in da se lahko morebitni neizbrisani osebni podatki in osebna korespondenca na vrnjenih delovnih sredstvih nepovratno uničijo z naključnim prepisovanjem in formatiranjem.

Z zadnjim dnem dela na UL se odhajajočemu zaposlenemu obvezno ukinejo vse dostopne pravice. Predal e-pošte zaposlenega, ki mu je prenehalo delovno razmerje na UL, se na poštnem strežniku hrani še najmanj 6 mesecev od dneva prekinitve delovnega razmerja oziroma po dogovoru. Po preteku dogovorjenega roka se predal e-pošte izbriše. Izjemoma se lahko e-poštni predal zaposlenega ohrani in nekateri dostopi do informacijskih sredstev UL, če zaposleni in UL podpišeta takšen dogovor, ki vsebuje elemente poglavja 4 Pogodbeno razmerje z zunanjimi izvajalci Politike varovanja odnosov s pogodbenimi izvajalci.

5.3 Ukrepi za zunanje sodelavce in izvajalce

Za vse zunanje sodelavce (pogodbeni sodelavci in študenti) se izvajajo enaki ukrepi kot za zaposlene.

6 DOLŽNOSTI ZAPOSLENIH

6.1 Spoštovanje informacijske varnostne politike

Vsi zaposleni so seznanjeni z vsebino Krovne politike, Politike informacijske varnosti in Operativnimi navodili.

6.2 Varovanje intelektualne lastnine

Zaposleni morajo varovati vse avtorske in sorodne pravice ter pravice intelektualne lastnine, ki pripadajo UL. Če pri opravljanju svojih delovnih obveznosti, zaposleni UL sodeluje s pogodbenimi izvajalci, morajo storiti vse potrebno, da se zavarujejo vse pravice intelektualne lastnine UL in so dolžni nemudoma prijaviti kakršne koli dogodke ali ravnanje, ki pomenijo kršitev teh pravic.

6.3 Varovanje zaupnih informacij

Zaposleni so dolžni varovati zaupne informacije, za katere izvedo med opravljanjem delovnega razmerja, tako med kot tudi izven delovnega časa, ter v ali izven prostorov UL. Informacije so dolžni varovati tudi po prenehanju delovnega razmerja.

6.4 Dajanje izjav javnosti

Izjave novinarjem oziroma javnosti lahko dajo zgolj s strani vodstva pooblaščene osebe.

7 USPOSABLJANJE ZAPOSLENIH

7.1 Izvajanje programov ozaveščanja, izobraževanja in usposabljanja

Za vse zaposlene in pogodbene izvajalce se načrtuje in izvaja program ozaveščanja, izobraževanja in usposabljanja o informacijski varnosti. Ob koncu izobraževanja lahko sledi preverjanje pridobljenega znanja.

Izobraževanje in usposabljanje glede informacijske varnosti je obveznost vseh zaposlenih.

Vsem zaposlenim je na razpolago dokumentacija, nanašajoča se na informacijsko varnost.

Vodstvo UL oziroma Skrbnik informacijske varnosti zaposlene redno obvešča o vseh pomembnih novostih in spremembah glede informacijske varnosti.

7.2 Izobraževanje administratorjev informacijskih sistemov

Administratorji se morajo redno izobraževati o vseh novostih, ki izhajajo iz njihovega delovnega razmerja ter jim omogočiti ustrezna orodja in pripomočke. Na osnovi pridobljenega znanja administratorji in skrbniki informacijskih sistemov dopolnjujejo postopke in navodila za varovanje. Na UL se stalno spremlja stanje na področju varovanja informacij, nova tveganja, ranljivosti ter nove varnostne tehnologije in se temu primerno tudi izobražuje.

8 VPOGLED/DOSTOP DO SLUŽBENIH INFORMACIJ ZAPOSLENEGA V IZREDNIH PRIMERIH

V izrednih primerih (nenadna odpoved zaposlenega, smrt delavca ali drug izreden dogodek) ima UL izrecno pravico dostopati le do uporabnikovih informacij in informacijskih sredstev, ki so službene narave. Namen in način vpogleda in dostopa podrobneje urejajo operativna navodila.

POLITIKA RAZVOJA PROGRAMSKE OPREME

1 POOBLASTILA IN ODGOVORNOSTI

Postavitev politike	Varnostni forum
Izvajanje	Redni zaposleni in zunanji izvajalci na UL, ki sodelujejo pri razvoju oziroma vzdrževanju programske opreme
Nadzor nad izvajanjem politike	Vodja službe za informatiko (tj. oseba, ki je odgovorna za delovanje službe za informatiko) oziroma drugi vodje OE
Komu je namenjena	Vsem redno zaposlenim in zunanjim izvajalcem na UL, ter ostalim, ki sodelujejo pri razvoju oziroma vzdrževanju programske opreme.

2 APLIKACIJSKA OKOLJA

Na UL ločimo naslednja programska okolja:

- razvojno, ki je namenjen lastnemu razvoju aplikacij za potrebe UL. Do razvojnega okolja lahko dostopajo izključno osebe, ki sodelujejo pri razvoju in vzdrževanju nove oziroma obstoječe programske opreme in izvedejo prvo fazo testiranja;
- testno, ki je namenjeno testiranju aplikacij za potrebe UL. Testno okolje je čim bolj podobno produkcijskemu okolju, v katerem se uporabijo podobni oziroma realni podatki iz produkcijskega okolja, kadar pa to zaradi zaupnosti informacij ni možno, pa s čim boljšim približkom realnim podatkom. Testiranje opravi testna skupina po vnaprej dogovorjenem načrtu, ki po končanju testiranja izdela poročilo. Ob pozitivnem poročilu se lahko aplikacija preseli v produkcijsko okolje. Ob negativnem poročilu pa testna skupina priloži k poročilu še ugotovitve in predloge za odpravo napak. Ob končanju testiranja se morajo tesni podatki uničiti.;
- produkcijsko je tisti del informacijskega sistema UL, ki služi dnevnim potrebam zaposlenih v standardnem okolju, komunikaciji med osebjem UL in komunikaciji UL s svojimi strankami, bančnimi ustanovami in tretjimi osebami. Aplikacijo se opremi z realnimi podatki, izobrazi uporabnike, namesti na strežnike in delovne postaje ter določi skrbnika informacije in skrbnika aplikacije.;
- izobraževalno je namenjeno zgolj za izvedbo tečajev oziroma izobraževanju uporabnikov te aplikacije.

Pri razvoju oziroma nabavi programske opreme UL sledi zakonskim zahtevam in ostalim predpisom, tako, da upošteva skladnost glede varovanja podatkov.

Postopki sprememb programske opreme za posamezno okolje so opisani v operativnih navodilih.

2.1 Osnovne zahteve pri prehajanju programske opreme aplikacij med okolji

Prehod programske opreme med posameznimi programskimi okolji mora biti nadziran in ustrezno dokumentiran. Pri tem se uporabljajo naslednje kontrole:

1. Ažuriranje programskih knjižnic in izvorne kode v produkciji sme izvajati le pooblaščeni skrbnik po pooblastilu vodje, ki je odgovoren za vzdrževanje aplikacije.
2. Izvršljiva koda se v produkcijsko okolje prenese šele:
   - ko je od uporabnikov pridobljena potrditev o uspešnem preverjanju in prevzemu,
   - ko so ažurirane ustrezne zbirke izvornih programov.
   - ali ko je drugače zagotovljeno, da izvedba kode ne more ogroziti varnosti podatkov v produkcijskem okolju.

3. Vzdržuje se dnevnik vpisov (*audit log*) za vse prehode programske opreme aplikacij med okolji.
4. Predhodne verzije programske opreme aplikacij se zadržijo (arhivirajo).
5. Prehodi med posameznimi okolji morajo biti ustrezno nadzirani in evidentirani.

2.2 Varovanje podatkovnih zbirk aplikacij

Dostop do podatkovnih zbirk mora biti nadzorovan z namenom zagotavljanja celovitosti podatkov in aplikacij. Kakršenkoli nepooblaščen dostop do podatkov in aplikacij mora biti onemogočen. Vse podatkovne zbirke so varovane z dostopnimi pravicami, to velja še posebej, če gre za zbirko podatkov, v katerih so občutljivi oziroma posebne vrste podatkov.

S tehničnimi sredstvi je zagotovljeno, da uporabniki testnega in produkcijskega okolja, ne morejo med okolji neposredno izmenjevati podatkov ali neovirano prehajati iz enega okolja v drugo.

2.3 Intervencija v produkcijskem okolju

V posebnih okoliščinah (kritična programska napaka, napaka v podatkih ipd.), ki onemogočajo delo in ne omogočajo normalnega vzdrževalnega ciklusa, je izjemoma mogoče dovoliti razvojnemu osebju neposredno poseganje v produkcijsko okolje. Skrbnik aplikacije, ki dovoli tak interventni poseg, je dolžan po takšnem posegu zamenjati geslo. Poseg se izvede preko posebnega uporabniškega dostopa, ki omogoči vse pravice na produkcijskem informacijskem sistemu. Podatki za interventni uporabniški dostop se hranijo na varnem mestu. Vse intervencijske posege mora izvajalec intervencije evidentirati v dnevniku interventnih posegov.

3 VPELJAVA SISTEMA

Novo programsko opremo je treba predhodno testirati v testnem okolju, ki je dokumentiran in potrjen s strani skupine, v katero so vključeni bodoči uporabniki in skrbniki informacijskega sistema, razen če je drugače zagotovljeno, da izvedba kode ne more ogroziti varnosti podatkov v produkcijskem okolju. Po uspešno opravljenem testu se lahko opravi prenos v produkcijsko okolje.

4 VZDRŽEVANJE APLIKACIJ

Vsaka sprememba mora biti pred samo uvedbo formalno odobrena s strani skrbnika oziroma vsebinskega skrbnika informacijskega sistema in preverjena/testirana v testnem okolju.

POLITIKA VAROVANJA ODNOSOV S POGODBENIMI IZVAJALCI

1 POOBLASTILA IN ODGOVORNOSTI

Postavitev politike	Varnostni forum
Izvajanje	Vse osebe, ki sodelujejo pri dogovorih in sklepanju pogodb s pogodbenimi izvajalci
Nadzor nad izvajanjem politike	Skrbnik informacijske varnosti
Komu je namenjena	Vsem zunanjim pogodbenim izvajalcem

2 PREPOZNAVANJE TVEGANJ PRI DOSTOPU POGODBEGA IZVAJALCA

Treba je oceniti tveganja in uvesti primerne kontrole za zmanjševanje tveganj, ki so povezana z dostopom pogodbenega izvajalca do informacijskih sredstev UL. Pri oceni tveganj je treba upoštevati:

- Zahtevani oziroma potrebni načini dostopa pogodbenega izvajalca do informacijskih sredstev UL (fizični, logični, oddaljeni dostop, lokacija dostopa),
- Vrednost, občutljivost in kritičnost informacijskih sredstev, do katerih bo dostopal pogodbeni izvajalec,
- Zahteve po izolaciji posameznih informacijskih sredstev, do katerih bo dostopal pogodbeni izvajalec, od ostalih informacijskih sredstev (zaščita informacij posameznih pogodbenih izvajalcev),
- Število, struktura in uporabniške pravice osebja pogodbenega izvajalca, ki bodo imele dostop do informacijskih sredstev UL,
- Postopek za avtorizacijo dostopov osebja pogodbenega izvajalca, postopek za preverjanje in pregledovanje pravic dostopov,
- Katere kontrole uporablja pogodbeni izvajalec za zaščito informacijskih sredstev, do katerih dostopa,
- Kakšne so posledice, če pogodbeni izvajalec ne more dostopati do informacijskih sredstev, oziroma so podatki nezanesljivi ali zavajajoči,
- Postopki za obravnavo varnostnih incidentov in postopki za zmanjševanje posledic incidentov,
- Zakonske zahteve in pogodbene obveze, ki jih je treba upoštevati pri ocenjevanju tveganj.

3 UVELJAVITEV POLITIK PRI POGODBENIH IZVAJALCIH

V odvisnosti od vrste storitve pogodbenega izvajalca in ocenjenih tveganj se na UL pripravi za posamezen pogodbeni odnos izvleček politik, ki vsebujejo pravila varovanja pri izvajanju pogodbeno dogovorjene storitve. Izvleček politik predstavlja obvezno prilogo k pogodbi s pogodbenim izvajalcem. Pogodbeni izvajalec mora biti s to politiko seznanjena in se zavezati k spoštovanju in upoštevanju dogovorjenih pravil.

4 POGODBENO RAZMERJE S POGODBENIMI IZVAJALCI

Pravno razmerje s pogodbenim izvajalcem se natančno opredeli s pogodbo, v kateri so določene vse potrebne varnostne zahteve. Pogodba predstavlja pravno podlago za dostop pogodbenega izvajalca do določenih podatkov oziroma informacijskih sistemov v okviru UL in njihovo uporabo. Projekti s strogo zaupnimi podatki se obravnavajo ločeno preko pogodb.

Pogodba s pogodbenim izvajalcem, ki je lahko, ali zunanji izvajalec ali naročnik informacijskih storitev (kupec) glede na predmet pogodbe vključuje vsaj naslednje elemente:

1. Izvleček politik, ki se nanašajo na zunanje izvajalce.
2. Kontrole za varovanje informacijskih sredstev:
   i. Postopki za varovanje informacijskih sredstev (informacije, programska in strojna oprema),
   ii. Potrebna fizična zaščita informacijskih sredstev,
   iii. Zaščita proti zlonamerni kodi,
   iv. Postopki za ugotavljanje izgube ali nepooblaščene spremembe informacij, programske ali strojne opreme,
   v. Postopek vračanja ali uničenja informacijskih sredstev ob prenehanju pogodbe,
   vi. Določitev zaupnosti, celovitosti in razpoložljivosti ter ostalih smiselnih značilnosti informacijskih sredstev,
   vii. Omejevanje kopiranja in širjenja informacij.
3. Potrebno uporabniško in skrbniško varnostno šolanje za vzpostavitev varnostnega zavedanja.
4. Določitev odgovornosti za nameščanje in vzdrževanje programske in strojne opreme.
5. Definiranje strukture in oblik poročanja ter obveščanja.
6. Postopek preiskave varnostnih dogodkov in kršitev.
7. Natančno določen proces upravljanja sprememb.
8. Politika upravljanja dostopov, ki določa:
   i. Razloge, zahteve in koristi, ki so potrebni za dodelitev dostopa pogodbenega izvajalca,
   ii. Način kontrole dostopa in identifikacije uporabnika pogodbenega izvajalca,
   iii. Postopek avtorizacije za dodeljevanje pravice dostopa do informacijskega sredstva,
   iv. Evidentiranje avtoriziranih uporabnikov za posamezen servis z definiranimi pravicami in privilegiji,
   v. Postopek za ukinjanje in ponovno vzpostavitev uporabniških pravic.
9. Opis storitve in predviden rok trajanja oziroma dobo opravljanja te storitve.
10. Opredelitev ciljnih ravni izvajanja storitev, vključno z opredelitvijo preverljivih kriterijev za doseganje teh ravni.
11. Določilo, da nedoseganje ciljne ravni opravljanja storitve, ki se ponavlja določen čas, šteje za kršitev pogodbe.
12. Pravico (varnostnega in revizijskega) pregleda in nadzorovanja pogodbenih obveznosti, lahko tudi s strani pogodbenih izvajalcev.
13. Definicija koračnega postopka za reševanje težav.
14. Zahteve za razpoložljivost storitve, ki vključujejo tudi zanesljivost izvajanja v skladu s poslovnimi prioritetami UL ter način vzdrževanja razpoložljivosti storitev v primeru naravne ali druge katastrofe.
15. Opredelitev obveznosti v zvezi s pravnimi zahtevami področne veljavne zakonodaje, kot so na primer predpisi na področju varovanja podatkov (npr. osebnih, tajnih,..) in varstva pravic intelektualne lastnine.
16. Način vključevanja podizvajalcev pogodbenega izvajalca in razširitev varnostnih zahtev tudi na podizvajalce.
17. Pogoji za preklic ali redefinicijo pogodbe:
   i. Pripravljen mora biti načrt za nadaljevanje delovanja tudi v primeru, če se predčasno prekine pogodba,
   ii. Predviden postopek za spremembo pogodbe v primeru spremembe varnostnih določil.
18. Po potrebi lahko UL vključi v pogodbo zahtevo po varnostnem preverjanju osebja pri pogodbenem izvajalcu, predvsem v primerih, ko bodo le-ti prihajali v stik ali delali z osebnimi podatki ter podatki, ki nosijo oznako zaupno in podobno.
19. Druge določbe, če so potrebne za čim bolj jasno definirano poslovno, organizacijsko, operativno, varnostno sodelovanje med izvajalcem in naročnikom.

POLITIKA UPRAVLJANJA SPREMEMB

1 POOBLASTILA IN ODGOVORNOSTI

Postavitev politike	Varnostni forum
Izvajanje	Redno in pogodbeno zaposleni na UL in vsem ostalim, ki na kakršenkoli način sodelujejo pri izvajanju sprememb na informacijskih sredstvih UL.
Nadzor nad izvajanjem politike	Skrbnik informacijske varnosti
Komu je namenjena	Redno in pogodbeno zaposlenim na UL in vsem drugim, ki na kakršenkoli način sodelujejo pri izvajanju sprememb na informacijskih sredstvih UL.

2 IZHODIŠČA UPRAVLJANJA SPREMEMB

Za zmanjševanje števila in negativnega vpliva napak v informacijskih sistemih UL je formaliziran proces upravljanja uvajanja sprememb v informacijske sisteme UL, ki mora zagotavljati vsaj naslednje elemente:

- evidentiranje vseh dogovorjenih aktivnosti (zahtevki, pooblastila ipd.),
- sprejemanje (obravnava) samo tistih zahtev, ki so odobrene s strani Varnostnega foruma,
- preverjanje zahtev v smislu ugotavljanja skladnosti z obstoječimi predpisanimi varnostnimi kontrolami in zahtevami,
- ugotavljanje, kateri programi, informacije in strojna oprema zahtevajo prilagoditev,
- pridobitev potrditve izvedbe spremembe pooblaščenega skrbnika, še preden se začne z izvedbo spremembe,
- tekoče (fazno) ažuriranje dokumentacije in ustrezno arhiviranje stare dokumentacije,
- kontrola verzij za vse nameščene programe v produkciji,
- obveščanje vseh odgovornih oseb o posamezni izvedeni spremembi.

Vse zahteve za spremembe ne glede na tip spremembe morajo biti formalizirane in odobrene s strani Varnostnega foruma za vsako aktivnost, ki lahko vpliva na izvajanje poslovnih procesov na UL. Pripadajoča dokumentacija spremembe se zbere in arhivira v centralnem arhivu v pisni ali elektronski obliki.

3 POSTOPKI UPRAVLJANJA SPREMEMB

Formalni proces upravljanja sprememb vključuje naslednje elemente:

1. Predvidene so tri ravni izvajanja procesa upravljanja sprememb,
   - postopek za izvedbo manj zahtevnih sprememb,
   - postopek za izvedbo zahtevnejših sprememb,
   - postopek za izvedbo nujnih sprememb.
2. Definiran je postopek za začetek procesa ter definirani merila za izbor ustrezne ravni upravljanja sprememb.

3.1 Manj zahtevne spremembe

Manj zahtevne spremembe so enostavnejše predvidljive spremembe, ki imajo vnaprej definirane postopke in potek aktivnosti in se ne pričakujejo negativne posledice na zagotavljanje informacijske podpore. Izvajanje manj zahtevnih sprememb se izvaja v okviru vnaprej predvidenih aktivnosti in odobrenih

pooblastil, ki so ustrezno dokumentirana oziroma jih lahko odobri neposredni vodja posamezne organizacijske enote.

3.2 Zahtevnejše spremembe

Zahtevnejše spremembe so spremembe, ki lahko povzročijo nepredvidljive posledice na poslovne procese, zato za njihovo pripravo in izvedbo obstaja postopek, ki zagotavlja sistematično ugotavljanje možnih vplivov ter primerno izvedbo spremembe, kot sledi.

Postopek za zahtevnejše spremembe je opisan v operativnih navodilih.

3.3 Nujne spremembe

Nujna sprememba je vsaka sprememba, ki se zaradi časovnih omejitev ne izvaja v skladu s postopki manj zahtevnih ali zahtevnejših sprememb. Nujne spremembe se izvajajo v primeru napak ter odprave posledic napake.

Nujne spremembe se izvajajo po interventnem postopku in jih mora odobriti skrbnik procesa. Kljub skrajšanemu postopku mora biti zaradi dokumentiranja spremembe, izdana in odobrena zahteva za spremembo. Za končano izvedbo spremembe se uporablja 3. točka prejšnjega poglavja – analiza izvedbe spremembe.

POLITIKA NEPREKINJENE INFORMACIJSKE VARNOSTI

1 POOBLASTILA IN ODGOVORNOSTI

Postavitev politike	Varnostni forum
Izvajanje	Vodja Službe za informatiko in vodje posameznih organizacijskih enot
Nadzor nad izvajanjem politike	Skrbnik informacijske varnosti
Komu je namenjena	IT osebju

2 VARNOST OSEBJA

V primerih, ko je ogroženo življenje, zdravje ali varnost oseb v prostorih ali pri poslovanju UL, se ne glede na določila te politike postopa tako, da se v največji možni meri varovati življenje in zdravje zaposlenih in študentov.

3 VARNOST INFORMACIJ

Neprekinjena informacijska varnost je vključena v proces upravljanja neprekinjenega poslovanja ali upravljanja obnove po neugodnih razmerah. Sistem neprekinjenega poslovanja zagotavlja obnovitev komunikacij in aplikativnih servisov po vnaprej določenem času, zlasti v primeru odpovedi sistema ali njegovega uničenja. UL ima za zagotovitev sistema neprekinjenega poslovanja informacijske tehnologije izdelan, redno vzdrževan in preverjen Načrt neprekinjenega poslovanja (NNP) in kot njegov sestavni del tudi Načrt za delovanje informacijskega sistema v primeru večje okvare oziroma nesreče. Vsaj 1 x letno se pregleda in uskladi NNP. Za vzpostavitev in vzdrževanje navedenih načrtov je odgovorno vodstvo UL, ki za nadzor s sklepom imenuje posebno delovno skupino.

Neprekinjeno poslovanje zagotavlja zunanji ponudnik certificirane e-hrambe, UL hrani gradivo kratkoročno in sama ne zagotavlja dolgoročne e-hrambe.

3.1 Analitični procesi za BCP-IT načrt

BCP (ang. Business continuity planning) - IT načrt upošteva realna tveganja, specifičnosti poslovnih procesov in zahtevane infrastrukture za njihovo podporo ter se v okviru določanja temeljnih izhodišč za BCP-IT načrt izvajajo naslednji procesi:

- analiza poslovnih procesov z določitvijo njihove kritičnosti za poslovanje ter definiranje zahtev za njihovo razpoložljivost,
- na osnovi rezultatov analize poslovnih procesov določitev dinamike vzpostavljanja delovanja procesov v rezervnem režimu,
- določitev kritičnih dogodkov z vplivom na poslovne procese z metodo analize tveganj,
- določitev osnovnih zahtev procesa BCP-IT načrt: lokacija, časovne zahteve za vzpostavitev BCP-IT načrt, popis vseh informacijskih sredstev, ki so potrebni za izvajanje poslovnega procesa in določitev zahtev za nujno infrastrukturo za delovanje BCP-IT načrta,
- izbor primernih rešitev glede na tveganja in osnovne zahteve BCP-IT načrt procesa.

Temeljna izhodišča BCP-IT načrta obravnava, preveri in potrdi Varnostni forum.

3.2 Vloge in odgovornosti za BCP-IT načrta

Za pripravo in izvajanje planiranja neprekinjenega poslovanja informacijske tehnologije je pristojna posebna delovna skupina, ki opravlja specifične naloge, ki se nanašajo na razvoj, vzdrževanje in testiranje BCP-IT načrta. V BCP-IT načrtu so vključene:

- jasno definirane in dokumentirane podrobnosti o nalogah načrta in nosilcih posameznih nalog,
- pooblastila nosilcem nalog in sledljivost uporabe pooblastil v neugodnih razmerah,
- definirane okoliščine, pod katerimi se naloge in določitev nosilcev nalog pregledujejo in revidirajo.

4 OSNOVNI POSTOPKI BCP-IT NAČRTI

BCP-IT načrt vsebuje opis naslednjih osnovnih postopkov:

- ob nastanku ugotavljanje velikosti in kritičnosti incidenta ter njegovih vplivih na delovanje kritičnih poslovnih procesov,
- postopek sprejemanja odločitve za prehod na rezervni režim,
- postopki prenosa poslovanja na rezervni režim v skladu s predvideno dinamiko reševanja kritičnih poslovnih procesov,
- delovanje v rezervnem režimu,
- sprejemanje odločitve in proces vrnitve v prejšnje stanje oziroma normalno delovanje.

5 IZDELAVA BCP-IT NAČRT PLANA

BCP-IT načrt vsebuje naslednje elemente:

- Dokumentirani opisi postopkov za izvajanje osnovnih BCP-IT načrt postopkov.
- Določitev posameznih nosilcev za izvajanje postopkov BCP-IT načrt.
- Identifikacija ponudnikov opreme in storitev za BCP-IT režime.
- Ureditev pogodbenih odnosov s ponudniki opreme in storitev.
- Načrt usposabljanja izvajalcev plana BCP-IT načrt.
- Plan preverjanja BCP-IT načrta:
    - Testiranje posameznih elementov plana.
    - Celovito testiranje plana v okviru internega IT sektorja.
    - Celovito testiranje z vključenostjo uporabnikov.

6 VZDRŽEVANJE BCP-IT NAČRT PLANA

BCP-IT načrt se posodobi v skladu s spremembami neugodnih poslovnih procesov oziroma IT tehnologij. BCP-IT načrt mora biti posodobljen nemudoma, ko se spremeni sistem ali oprema, ki povzroči, da obstoječi BCP-IT načrt ne drži več. Posodobitev lahko sproži:

- nabava nove opreme ali dopolnitev informacijskega okolja,
- uvajanje novih tehnologij,
- spremembe v osebju ali organizaciji,
- spremembe pogodbenih strank ali dobaviteljev,
- spremembe oziroma uvajanje novih neugodnih poslovnih procesov,
- spremembe v zakonodaji, ki imajo vpliv na načrt,
- spremembe v načinu obratovanja.

Ne glede na spremembe sistema mora biti BCP-IT načrt pregledan in posodobljen vsaj enkrat letno.

7 VADBA IN TESTIRANJE BCP-IT NAČRT

Za uspešno izvajanje postopkov BCP-IT načrt v realnih razmerah je treba vaditi in preverjati BCP-IT načrt. Testiranje postopkov se izvaja periodično, najmanj enkrat letno. Za testiranje mora biti na voljo ustrezna oprema in človeški viri.

POLITIKA FIZIČNEGA VAROVANJA

1 POOBLASTILA IN ODGOVORNOSTI

Postavitev politike	Varnostni forum
Izvajanje	Vsi zaposleni (redno in pogodbeno zaposleni, zunanji sodelavci, stranke itd.)
Nadzor nad izvajanjem politike	Skrbnik informacijske varnosti
Komu je namenjena	Vsi, ki imajo pravico dostopa do informacijskih sistemov

2 OPREDELITEV GROŽENJ

Fizično varovanje pokriva področje naslednjih kategorij groženj:

- Ogrožanje (uničenje, razkritje, poneverjanje ali onemogočanje) informacijskih sredstev z neposrednim fizičnim dostopom ali kontaktom;
- Uničenje informacijskih sredstev v požaru, izlivu vode ali padcu z višine;
- Onemogočanje informacijskih sredstev z onemogočanjem podpornih infrastrukturnih sistemov;
- Ogrožanje informacijskih sredstev zaradi malomarnosti in neustreznega ravnanja.

3 UKREPI FIZIČNEGA VAROVANJA

UL izvaja organizacijske, tehnične in druge ukrepe za preprečevanje oziroma zmanjšanje neposrednega fizičnega ogrožanja informacijskih sredstev, skladno s Hišnim redom.

V primerih, ko bi bilo ogroženo življenje, zdravje ali varnost oseb v prostorih UL, se v največji možni meri zaščiti najprej življenje in zdravje osebja.

4 OPREDELITEV VARNOSTNIH PODROČIJ

Fizično varovanje mora biti v vseh prostorih UL sorazmerno z ravnijo ogroženosti informacijskih sredstev oziroma poslovanja UL. Glede na ogroženost so varovana območja, razporejena v tri varnostna področja:

- Visoka raven varovanja, to so prostori, kjer obstaja možnost prekinitve poslovanja za celotno UL in posamezna informacijska sredstva (sistemski prostor, administratorski prostor) ter področja, za katera zakonodaja zahteva visoko raven varovanja. ;
- Srednja raven varovanja, to so prostori, kjer obstaja možnost dostopa in ogrožanja posameznih informacijskih sredstev, katerih ogrožanje pa ne pomeni prekinitve izvajanj poslovnih funkcij, a pomeni škodo za posamezne poslovne funkcije UL (pisarne zaposlenih, arhivi);
- Nižja raven varovanja, to so prostori, ki služijo splošnemu namenu in ne obstaja neposredna možnost ogrožanja informacijskih sredstev (hodniki, stopnišče, sanitarije, vstopni prostor).

4.1 Dostop v visoko varovane prostore

Vstop v visoko varovane prostore je dovoljen in omejen le pooblaščenim zaposlenim UL v času in obsegu za opravljanje obveznosti iz delovnega razmerja. Vsak dostop v visoko varovane prostore je ustrezno evidentiran in dokumentiran.

V okviru UL se evidentirajo in klasificirajo vse lokacije, v skladu s pomembnostjo oziroma ogroženostjo. Za vsak visok varovan prostor se formalno določi skrbnika, ki skrbi za ustrezno raven varovanja ter morebitna dodatna pravila, ki veljajo za ta prostor.

4.1.1 Sistemska soba

Dostop do sistemske sobe je dovoljen odgovornim osebam za delovanje informacijskega okolja UL, skrbniku informacijske varnosti, vodji Službe za informatiko in drugim zaposlenim na UL, ki imajo za to pisno pooblastilo vodstva ali nadrejenega. Dostop do sistemske sobe je mogoč s ključem ali elektronsko kartico, ki je dodeljena naštetim osebam.

Osebe, ki niso zaposlene na UL (npr. vzdrževalci prostorov, strojne in programske opreme, obiskovalci, pogodbeni izvajalci) smejo vstopiti v sistemsko sobo v prisotnosti vsaj ene od oseb iz 1. odstavka tega poglavja, razen v izrednih primerih (varnostna služba v primeru suma vloma in/ali požara).

Vsak vstop v sistemsko sobo se mora zabeležiti. Priporoča se beleženje datuma vstopa, ime in priimek osebe, ki je vstopila ter namen vstopa oziroma opravljeni posegi. Vstopi v sistemsko sobo se beležijo v za to namenjeni evidenci na papirnem obrazcu, ki se nahaja v sistemski sobi in/ali elektronsko vodeni evidenci vstopov z elektronsko kartico, ki beleži številko kartice, datum in čas vstopa. Evidenco vstopov v sistemsko sobo redno pregleduje (najmanj enkrat letno) skrbnik informacijskega okolja UL.

4.1.1.1 Klimatska naprava in električno napajanje

Sistemska soba se varuje z varnostnimi ukrepi in postopki za zaščito pred okoljskimi nevarnostmi, in sicer s klimatskimi napravami za zagotavljanje ustreznega temperaturnega območja, sistemom za nadzor temperature, gasilnimi aparati in sistemom UPS za neprekinjeno napajanje.

Računalniška oprema (strežniki, diskovna polja, delovne postaje in druga oprema) mora biti nameščena v pogojih, ki so skladni s tehničnimi specifikacijami proizvajalca opreme. Ustreznost delovanja varnostnih naprav preverjajo skrbniki informacijskega okolja UL periodično in o tem vodijo zapisnik. Vsi varnostni ukrepi in naprave morajo delovati v vsakem trenutku (tudi izven delovnega časa).

Električna in telekomunikacijska napeljava mora biti nameščena tako, da je ni možno nenamerno prekiniti ali brez večjih težav uničiti ali zlorabiti.

4.2 Glede na požarni red UL

Prepovedana je uporaba lahko vnetljivih ali eksplozivnih materialov v prostorih UL, razen v za ta namen določenih in primerno opremljenih mestih.

Prepovedano je kuhanje in uporabe posebnih grelnih teles v prostorih UL, razen v za to posebno določenih in opremljenih prostorih UL.

V primeru požara se ravna skladno z internimi akti, ki urejajo ukrepanje v primeru požarne nevarnosti.

4.3 Ostali organizacijski ukrepi

Vzdrževanje elementov tehničnega varovanja je dogovorjeno in izvajano v obsegu, ki zagotavlja nemoteno in pravilno delovanje posameznega tehničnega elementa. Vsa varnostna oprema se mora redno pregledovati skladno z navodili proizvajalca.

Snemanje prostorov najvišjega ali visokega varnostnega področja UL z avdio in video snemalnimi napravami s strani zaposlenih ali zunanjih oseb je dovoljeno le s posebnim dovoljenjem. Fotografska oprema, kasetofoni in videorekorderji se ne smejo puščati v teh prostorih, razen s posebnim dovoljenjem. Vsi postopki ob nevarnostih morajo biti dokumentirani in se periodično preverjati in testirati.

Rezervna oprema in rezervne kopije nosilcev podatkov morajo biti varno shranjeni na varnem mestu na lokaciji, različni od lokacije sistemskega prostora. Prav tako mora biti zagotovljeno ustrezno varovanje v času transporta do ali z varnega mesta, kjer se hranijo.

5 TEHNIČNI UKREPI IN VAROVANJE PODROČIJ VISOKE ZAŠČITE

5.1 Protipožarno varovanje

Avtomatski požarni alarmi sistem mora imeti z ustrezno lokalno zvočno signalizacijo in opozarjanjem pogodbeno vezane varnostne službe.

Gasilni aparati morajo biti nameščeni na vseh mestih, kjer je to opredeljeno s požarnim elaboratom in požarnim redom in so redno vzdrževani.

5.2 Protipoplavna varnost

Na področjih, kjer lahko pride do ogrožanja poslovanja zaradi izliva vode, se uporabljajo javljalniki izliva vode z avtomatskimi elektromagnetnimi ventili in javljalnikom.

5.3 Protivlomno varovanje

Za varovanje izven poslovnih ur UL se v prostorih, kjer ni zagotovljenega neprekinjenega režima dela, uporablja protivlomni alarmni sistem s senzorji, videonadzorom in z avtomatskim alarmiranjem varnostne službe.

5.4 Fizična kontrola dostopa

Varovano območje je zavarovano z ustreznimi vhodnimi kontrolami, ki zagotavljajo, da je dostop dovoljen le pooblaščenim osebam. Pri tem se upošteva:

- Za vstop v varovane prostore morajo biti formalno določene pooblaščene osebe za reden delovni čas ter posebej za izven rednega delovnega časa. Ob vstopu in izhodu iz posebej varovanih prostorov se zagotovi kakovostna identifikacija pooblaščenih oseb s sprejemljivimi identifikacijskimi metodami oziroma njihovo kombinacijo;
- Dostop do varovanih prostorov mora biti omejen z vsaj eno fizično oviro, ki bo zahtevala ustrezno identifikacijo osebe ter avtorizirala uporabo prehoda z izbrano identifikacijsko metodo;
- Identificiranje in prehodi preko varnostnih ovir se elektronsko evidentirajo;
- Vsak obisk nepooblaščenih oseb mora biti evidentiran z osebnimi podatki, datumom in uro prihoda in odhoda, namen obiska in morebitnim imenom spremljevalca;
- Ob prehodu mimo fizičnih ovir je zaposleni, ki se je identificiral in zahteval, ali odobril prehod, dolžan zagotoviti, da ne pride do prehajanja oseb, ki nimajo dovoljenega dostopa do posameznega varnostnega območja;
- Za potrebe evidentiranja dostopa do posameznih varnostnih območij in za izvajaje nadzora se uporablja video nadzor in snemanje. Način in obseg pregledovanja tako zbranih informacij se izvajata na podlagi odločitve Varnostnega foruma.

6 POSEBNI UKREPI FIZIČNEGA VAROVANJA

V primeru neposrednega fizičnega ogrožanja zaposlenih UL in/ali informacijskih sredstev se izvede dodatno zavarovanje prostorov z varnostnikom ali s prisotnostjo policije, ki se izvede v delovnem času s pozivom intervencijske enote varnostne službe ali policije oziroma izvedel delovnega časa preko avtomatskega protivlomnega in protipožarnega varnostnega sistema z avtomatskim alarmiranjem. Po vsakem posredovanju in aktiviranju intervencijske enote mora biti izdelano poročilo.

PRILOGA 1: REFERENČNI - URADNI DOKUMENTI

SUVI na UL upošteva najmanj naslednje standarde, priporočila in zakone s pripadajočimi podzakonskimi akti:

Slovenski zakoni:
- Zakon o varstvu osebnih podatkov
- Zakon o visokem šolstvu
- Zakon o elektronskih komunikacijah
- Zakon o elektronskem poslovanju in elektronskem podpisu
- Zakon o avtorskih in sorodnih pravicah
- Zakon o elektronskem poslovanju na trgu
- Zakon o varovanju dokumentarnega in arhivskega gradiva ter arhivih

Standardi:
- mednarodni standard - ISO/IEC 27000
- mednarodni standard - ISO/IEC 27001
- mednarodni standard - ISO/IEC 27002
- mednarodni standard - ISO/IEC 17799
- mednarodni standard - ISO 22301
- slovenski računovodski standardi
- mednarodni standardi računovodskega poročanja

Interni akti s področja varovanja:
- Pravilnik o varovanju osebnih in zaupnih podatkov na UL
- Pravila uporabe omrežja Metulj
- Priporočila članicam za priklop v univerzitetno omrežje Metulj
- Priporočila članicam za ureditev sistemskega prostora
- Pravilnik o prijavljanju težav in potreb, povezanimi z informacijsko komunikacijskimi storitvami in računalniško opremo
- Operativna navodila.