

Informacijska varnostna politika za uporabnike

Vsebina

1. UVOD	3
2. SPLOŠNA VARNOST IN ZAHTEVE ZA UPORABO	4
2.1 DOVOLJEN NAČIN UPORABE RAČUNALNIŠKE OPREME	4
2.2 ZAKONODAJA	4
2.3 ZAŠČITA INFORMACIJ	5
2.4 LOKALNO RAČUNALNIŠKO OMREŽJE	6
2.5 ZUNANJE POVEZAVE IN ODDALJENI DOSTOP	6
2.6 ELEKTRONSKA POŠTA IN INTERNET	7
3. VARNOSTNE ZAHTEVE ZA DELOVNE POSTAJE	11
3.1 VARNOST DELOVNE POSTAJE	11
3.2 VARNOST MOBILNIH NAPRAV	11
3.3 ZLONAMERNA PROGRAMSKA OPREMA	11
3.4 POŽARNA PREGRADA	12
3.5 DOSTOP DO DELOVNE POSTAJE	12
4. SPOROČANJE VARNOSTNIH INCIDENTOV	13
5. PREHODNE IN KONČNE DOLOČBE	14

1. Uvod

Dokument »Informacijska varnostna politika za uporabnike« vsebuje javne informacije, ki po klasifikaciji dokumentov ne potrebujejo posebne oznake. Z informacijami tega dokumenta morajo biti seznanjeni vsi uporabniki informacijskega sistema UM.

Dokument opisuje osnovne informacijske varnostne mehanizme, ki jih morajo poznati in spoštovati vsi zaposleni na UM, poslovni partnerji in ostali uporabniki informacijskega sistema UM.

Dokument obravnava odgovornosti vseh zaposlenih in drugih uporabnikov za zaščito informacij in infrastrukture UM in najpomembnejše postopke za zaščito delovnih postaj ter zaščito pred zlonamernimi programi.

Natančna navodila za implementacijo v tem dokumentu definiranih zahtev so opisana v ustreznih organizacijskih predpisih.

Nespoštovanje zahtev, opisanih v tem dokumentu, pomeni kršitev delovnih oz. pogodbenih in študijskih obveznosti.

Pri ostalih uporabnikih storitev UM, ki niso pogodbeno vezani z UM, je pristojnost RCUM ali da omeji ali odvzame dostop.

Dokument se pregleduje letno. V primeru predlaganih sprememb dokumenta varnostni inženir opravi pregled vseh predlaganih sprememb in pripravi končni predlog sprememb dokumenta.

2. Splošna varnost in zahteve za uporabo

2.1 Dovoljen način uporabe računalniške opreme

2.1.1 Postavitev in konfiguracija delovne postaje za zaposlene

Postavljanje in premeščanje stacionarne računalniške informacijske opreme uporabnikom in nepooblaščenim osebam ni dovoljeno.

Spreminjanje nastavitve delovne postaje (npr. spreminjanje parametrov dostopa do interneta, izklapljanje protivirusne zaščite, požarne pregrade, ...) s strani uporabnika ali druge nepooblaščen osebe določajo predpisi za posamezno članico UM.

2.1.2 Uporaba računalniške opreme in infrastrukture UM v zasebne namene in uporaba zasebne računalniške opreme

Uporaba računalniške informacijske opreme in infrastrukture UM, je namenjena samo za nekomercialno uporabo (pedagoška, raziskovalna raba) in projekte, ki se izvajajo v okviru UM.

Uporaba zasebne računalniške opreme je dovoljena v skladu s pravili uporabe, ki jih določa RCUM.

2.1.3 Uporaba interneta in elektronske pošte

Uporaba elektronske pošte in interneta se dovoljuje in omejuje v skladu s politiko UM in se regulira v smislu večanja varnosti in zmanjševanja informacijskih incidentov. Vse systemske uporabniške aktivnosti se beležijo z namenom zagotavljanja nemotenega delovanja informacijskega sistema. Vsebina uporabniških aktivnosti, t.j. vsebina uporabnikovih paketov (vsebina e-pošte, vsebina priponk, vsebina obiskov internetnih strani), se ne beleži ali kako drugače spremlja.

Kakršno koli časovno omejeno pregledovanje šifriranega prometa SSL za znane ciljne naslove z namenom odkrivanja zlorab je dovoljeno le ob prehodnem obvestilu uporabnikov. V tem primeru je potrebno uporabnikom poslati po e-pošti natančno obvestilo o trajanju in obsegu pregledovanja, kar se mora objaviti tudi na spletni strani univerze in RCUM.

V primeru neobičajnega obnašanja informacijskega sistema je uporabnik dolžan obvestiti odgovorno osebo za informacijsko varnost na UM in ravnati po njihovih navodilih. RCUM vodi evidenco informacijskih incidentov, ki jo redno pregleduje odgovorna oseba za informacijsko varnost in izvaja ustrezne varnostne ukrepe.

2.2 Zakonodaja

2.2.1 Licence programske opreme

Posebna skrb mora biti posvečena pri uporabi programske opreme, ki je kot intelektualna lastnina zaščitena z avtorskimi pravicami. Pred nameščanjem programske opreme se lahko uporabnik posvetuje s skrbniki informacijskih sistemov.

Če uporabnik potrebuje programsko opremo, ki ni del standardne, se za nakup in nameščanje opreme dogovori s predpostavljenim, pri čemer sam odgovarja zanjo.

Uporaba programske opreme, pridobljene na nelegalen način, je prepovedana.

2.2.2 Avtorske pravice in intelektualna lastnina

Večina informacij in programske opreme (glasba, video, programi, filmi, dokumenti, ...), ki so dostopni v javni domeni (vključno z internetom), je zaščiten z avtorskimi pravicami ali drugo obliko zaščite intelektualne lastnine. S kršenjem avtorskih pravic in intelektualne lastnine posameznik prevzame vso materialno in kazensko odgovornost. V primeru dvomov o možnosti uporabe materialov se je potrebno posvetovati s pristojno službo.

2.2.3 Varovanje zasebnosti

UM zbira in vzdržuje osebne informacije, ki so zbrane v zbirkah, ki so objavljene v registru zbirk osebnih podatkov pri informacijskem pooblaščenču.

Osebne datoteke, informacije in podatke je potrebno vedno hraniti na za to predpisanih informacijskih sredstvih, ki so zavarovana. Postopki varovanja so podrobneje določeni v pravilniku, ki ureja to področje - Pravilnik o zavarovanju osebnih in zaupnih podatkov št. A11/2006-524 JR.

Zaposleni ne smejo dostopati do informacijskih sredstev drugih zaposlenih (npr. datotek, zapisov, drugih vsebin na različnih napravah in v fizični obliki) brez predhodne odobritve lastnika oz. skrbnika (v primeru osebnih podatkov brez privolitve posameznika).

2.3 Zaščita informacij

2.3.1 Gesla

Geslo v povezavi z uporabniškim imenom za računalniški dostop je glavni način identifikacije in posledično omogoča dostop do informacijskih virov UM. Za lastno zaščito in za zaščito informacijskih sredstev in virov UM mora biti geslo tajno in ga ni dovoljeno deliti z drugimi.

Na sistemih UM in aplikacijah je potrebno za postavljanje gesel in pri njihovem rokoivanju upoštevati pravila, ki jih objavi RCUM na svoji spletni strani.

Gesla so obravnavana kot zaupne informacije. Uporabnik je dolžan skrbeti za tajnost svojega gesla, tako da:

- ga ne deli ali razkrije drugim uporabnikom,
- ga ne sporoča po telefonu,
- ga ne razkrije (npr. vodji, administratorju ali skrbniku računalniškega informacijskega sistema),
- ne uporablja možnosti shranjevanja gesel v aplikacijah, ki to omogočajo,
- si ga ne zapisuje,
- ga ne shranjuje v informacijskih sredstvih (računalnik, dlančnik, mobilni telefon ipd.),
- uporablja taka službena gesla, ki niso enaka geslom, ki se uporabljajo v zasebne ali druge namene.

Šifrirna gesla za informacijska sredstva se uporabljajo za zaščito pred nedovoljenim dostopom in ne za identifikacijo. Zato ta gesla sporočimo nadrejenemu, ki jih shrani v zapečateni kuverti na varnem mestu.

Pri dostopu do informacijskih virov, ki niso pod kontrolo UM (domači računalniki, privatni elektronski predal, ...), ni dovoljeno izbirati istih gesel kot za dostop do informacijskih virov na UM.

2.3.2 Varovanje zaupnih informacij

Vse informacije na UM so opredeljene kot je določeno v Pravilniku o zavarovanju osebnih in zaupnih podatkov št. A11/2006-524 JR.

Zaupne informacije UM morajo biti varovane pred nepooblaščenim dostopom, pregledom in spreminjanjem:

- Zaupne informacije UM morajo biti praviloma šifrirane ob pošiljanju izven omrežja UM.
- Zaupne informacije na prenosnih medijih (diskete, CD, USB ključi...) je potrebno označiti kot zaupne in hraniti v ustreznih prostorih ali omarah.
- Zaupne informacije UM ne smejo biti shranjene na računalnikih, ki niso v lasti UM.
- Pri tiskanju zaupnih informacij UM je dovoljeno uporabljati le interne tiskalnike. Tiskani material je potrebno takoj pobrati in varno hraniti.
- Zaposleni morajo upoštevati načelo čiste mize. Ta določa, da ni dovoljeno puščati materialov z zaupnimi informacijami na mizi v času svoje odsotnosti. Zaupne materiale je potrebno hraniti v zaklenjenih predalih, omarah ali sobi.
- Po prenehanju uporabe natisnjenih dokumentov oz. drugih medijev, ki vsebujejo zaupne informacije, je potrebno medije fizično uničiti ali podatke izbrisati na način, ki onemogoča obnovitev izvirnih informacij (razrez tiskanih medijev, fizično uničenje nosilcev kot so CD, DVD, večkratni prepis pomnilniškega medija z naključnimi vrednostmi).

2.3.3 Varovanje zaupnih podatkov poslovnih partnerjev

V okviru običajnega poslovanja se na UM zbirajo tudi informacije o drugih organizacijah in poslovnih partnerjih. Te informacije so namenjene izključno poslovni rabi in so opredeljene kot zaupne.

2.4 Lokalno računalniško omrežje

Ob priklopu na lokalno računalniško omrežje UM je potrebno upoštevati naslednje zahteve:

- na omrežju se ni dovoljeno predstavljati kot nekdo drug (maskiranje),
- prisluškovanje omrežnemu prometu ni dovoljeno,
- poganjanje sistemskih in varnostnih aplikacij na sistemih ni dovoljeno, razen pooblaščenim osebam,
- dodajanje mrežnih naprav, ki razširjajo infrastrukturo UM (stikalo, usmerjevalnik, hub, modem, brezžična dostopna točka, ...) ni dovoljeno, razen pooblaščenim osebam. Uporabnik, ki dodaja mrežne naprave v omrežje UM, je odgovoren za njihovo uporabo in prav tako za dejavnosti vseh uporabnikov, ki so priključeni na to napravo.

V primeru uporabe drugih omrežij v prostorih UM se je potrebno predhodno posvetovati in upoštevati navodila informacijskega varnostnega inženirja in RCUM-a, ki določi pogoje za uporabo druge opreme (predvsem velja za opremo, ki omogoča brezžičen dostop).

2.5 Zunanje povezave in oddaljeni dostop

2.5.1 Zunanje povezave

Priklop sistemov ali omrežij na druge sisteme ali omrežja, vključno z internetom, ali direktne povezave, predstavlja za UM varnostno grožnjo, zato veljajo sledeče zahteve:

- dostop do drugih omrežij je dovoljen le na sistemsko odobren način, ni dovoljen mimo varnostnih mehanizmov zaščite UM,
- pred priključitvijo na informacijske sisteme ali omrežje UM iz zunanjih omrežij mora biti uporabnik registriran in mora uporabiti dovoljene *vhodne točke*. Dostop se uredi na pisno zahtevo in ob odobritvi odgovorne osebe.

2.5.2 Oddaljen dostop do virov UM

Zaposleni na UM lahko dostopajo do informacijskih virov na daljavo preko splošno dostopnih komunikacijskih poti in uporabi šifrirane povezave do omrežja UM.

Pri delu na daljavo, kjer ne uporabljamo informacijskih sredstev v lasti UM in za katere ne skrbi UM, je potrebno upoštevati:

- na informacijsko napravo ne prenašamo informacijskih vsebin, ki so označene kot zaupne,
- če za oddaljen pristop uporabljamo spletni brskalnik, ga po končanem delu zapremo in pobrišemo vse delovne procese-aplikacije,
- vse delovne dokumente, ki smo jih ustvarili na oddaljenem informacijskem sredstvu izbrišemo in zapremo aplikacije.

2.6 Elektronska pošta in internet

2.6.1 Uporaba storitev elektronske pošte

Do elektronskega predala UM so upravičeni vsi zaposleni na UM, zaslužni profesorji UM ter tisti, ki imajo pogodbo o zaposlitvi na UM v mirovanju. Vsem tem se na univerzitetnem strežniku za e-pošto omogoči uporaba elektronske pošte v obliki, ki tipično ime.priimek@um.si. Izjeme nastopijo v primerih, ko obstaja več oseb z istim imenom ali priimkom, ko skupna dolžina imena in priimka presega 20 znakov ali drugih utemeljenih razlogih. Vir podatkov o uporabniku je kadrovske informacijski sistem UM.

Z dnem prekinitve delovnega razmerja se odvzame pravica do uporabe informacijskih sredstev, vključno z e-naslovom in ukinejo vsi dostopi do informacijskih virov. Opuščene identitete (e-naslava) ni dovoljeno spet ponovno uporabiti za drugega uporabnika.

Upokojenim (bivši visokošolski učitelji in sodelavci ter administrativno osebje, ki se je upokojilo na UM) se na zahtevo dodeli naslov elektronske pošte ime.priimek@guest.um.si (veljajo omejitve iz prejšnjega odstavka) na univerzitetnem strežniku za e-pošto, na katerega se preusmeri elektronska pošta z elektronskega naslova UM, ki je veljal pred upokojitvijo. Vir podatkov o uporabniku je informacijski sistem UM.

Elektronski naslov oblike ime.priimek@guest.um.si se omogoči za druge sodelujoče z UM, kjer obstaja za sodelovanje pravna podlaga s finančnim učinkom. V tem primeru vlogo, ki jo pripravi predlagatelj, ki je nekdo izmed zaposlenih na UM, odobri dekan ali rektor. Odgovornost predlagatelja je, da poskrbi, da se ob zaključku sodelovanja elektronski račun ukine, da ne pride do neupravičene uporabe sredstev UM. Opustitev takega dolžnega ravnanja se šteje za kršitev delovnih obveznosti.

Študentom se dodeli elektronski naslov oblike, ki je tipično ime.priimek@student.um.si (veljajo omejitve iz prvega odstavka tega člena). Vir podatkov o uporabniku je akademski informacijski

sistem. Pravica do uporabe informacijskih sredstev UM s strani študentov je povezana s statusom, ki ga ima posamezni študent. Opuščene identitete (e-naslova) ni dovoljeno spet ponovno uporabiti za drugega uporabnika.

Osebam, ki v posameznem študijskem letu nimajo statusa študenta in želijo opraviti oziroma dokončati študijske obveznosti, se po odobritvi pristojnega referata za študijske zadeve, ki obravnava individualno zaprosilo študenta, odobri dostop do informacijskih sredstev UM največ do konca študijskega leta. V teh primerih lahko Univerza v Mariboru zaračuna strošek dodelitve dostopa in uporabe informacijskih sredstev UM. V takem primeru Upravni odbor Univerze v Mariboru določi višino nadomestila za dostop do informacijskih storitev UM .

Za druge potrebe, kot so: organizacijske enote, posamezni projekti, pomoč uporabnikom in podobno, se lahko odprejo institucionalni oziroma namenski predali oblike institucija@um.si. Elektronska sporočila, ki prispejo v take predale, uporabljajo in upravljajo pooblaščen uporabniki. Znana mora biti odgovorna oseba.

Veljajo tudi naslednja pravila:

- elektronski naslovi za fizično osebo morajo biti oblike *ime.priimek@[guest,student].um.si* . Ime je lahko tudi krajše kot uradno ime in je lahko tako, kot ga oseba uporablja (Nikolaj – Niko, Aleksander - Sašo).
- Anonimnih elektronskih naslovov na UM ni.
- Dodeljen elektronski predal se uporablja za komunikacijo znotraj UM. Uporaba drugih elektronskih predalov uporabnika je za komunikacijo znotraj in v imenu UM nezaželen.
- Skrbnik sistema elektronske pošte UM je RCUM, ki sme posamezna administrativna opravila poveriti skrbnikom članic.
- Skrbnik sistema elektronske pošte kreira in ureja uporabniške poštno predale na zahtevo pristojnih oseb, ki mu posredujejo vse potrebne podatke.
- V primeru prenehanja uporabe ali ukinitve uporabniškega predala se ukine e-poštni naslov, kar lahko pomeni tudi ukinitve dostopa do domenskih storitev. Vsebina predala se izbriše po preteku treh mesecev od dneva zaprtja predala. Do zaprtja predala lahko uporabnik sam poskrbi za prenos/zaščito vsebine, po zaprtju pa za zaščito vsebine poskrbi skrbnik sistema elektronske pošte.
- Preusmeritev elektronskih sporočil uporabnika v predal izven informacijskega sistema UM iz razlogov zagotavljanja razpoložljivosti ni dovoljena.

Uporaba poštnega predala

Vsak uporabnik elektronske pošte ima svoj elektronski predal. Za druge potrebe, kot so: organizacijske enote, posamezni projekti, pomoč uporabnikom in podobno; se odprejo namenski predali. Elektronska sporočila, ki prispejo v namenske predale, uporabljajo in upravljajo pooblaščen uporabniki.

Uporabnik ne sme uporabljati predala v neslužbene namene kot so pridobitna dejavnost, neslužbene (ankete in vprašalniki, trgovina, ipd.) in politične aktivnosti. Prepovedano je razpošiljanje vseh vrst neželene pošte.

Priporočila:

Elektronska sporočila naj bodo kratka z malo priponk. Velikost poslane ali sprejete elektronske pošte skupaj s priponkami je omejena. V primeru, da je omejitev presežena, se sporočilo avtomatično

zavrne. Pošiljatelj dobi obvestilo o zavrnitvi. Omejitev je preventivni ukrep za preprečevanje prekomernega obremenjevanja sistema.

Če uporabnik po pomoti prejme sporočilo, ki mu ni namenjeno, vsebine tega sporočila ne sme shraniti ali uporabljati za katerikoli namen. O pomoti je dolžan nemudoma obvestiti pošiljatelja in prejeto sporočilo takoj izbrisati.

Pošiljanje in prejemanje elektronskih sporočil

Pri pošiljanju elektronskih sporočil mora uporabnik upoštevati načelo racionalnosti in varnosti. Obsežnih priponek naj se ne pošilja, če pa že, naj se jih pretvori v ustrezeni format, ki omogoča stiskanje vsebine. Iz varnostnih razlogov dokumentov s končnicami, ki omogočajo avtomatsko izvajanje, ni priporočljivo prenašati z elektronsko pošto.

Uporabnik se ne sme prijavljati s službenim naslovom na elektronske poštno sezname, če ti niso vsebinsko povezani z delovnimi nalogami uporabnika ali uporabljati službeni naslov elektronske pošte kot podatek pri izpolnjevanju elektronskih obrazcev, če ti niso vsebinsko povezani z delovnimi nalogami uporabnika.

Uporabnik ne sme preusmerjati elektronskih sporočil.

Brisanje elektronskih sporočil

Uporabnik mora vzdrževati svoj elektronski poštni predal tako, da po potrebi, ki jo narekujejo omejitve kapacitete ali druge omejitve, arhivira in izbriše vsa elektronska sporočila, ki jih ne potrebuje več v službene namene ali so zasebne narave.

Skrbnik se lahko odloči za ukrepanje v primeru, če bi uporabnik:

- uporabljal elektronsko pošto za pošiljanje verižnih pisem,
- uporabljal elektronsko pošto za prenos množičnih sporočil ("spamming").

V primeru nedovoljene uporabe sistema za elektronska sporočila, lahko skrbnik začasno onemogoči uporabo sistema za uporabnika.

2.6.2 Uporaba storitev na internetu

Uporabnikom je dostop do interneta omogočen za njihovo delo in izobraževanje. Uporabnik se mora obnašati racionalno in internet uporabljati kot delovni pripomoček. Omrežje UM je povezano z omrežjem internet preko povezave, ki jo zagotavlja ARNES, zato je potrebno upoštevati pravila dopustne rabe, ki jo predpisuje ARNES¹.

Pri uporabi storitev v oblaku, ki omogočajo shranjevanje podatkov in omrežij, ki omogočajo komunikacijo »vsakega z vsakim« (angl. peer to peer) je potrebno upoštevati pravila, ki jih objavi RCUM. Promet pri uporabi prenosa datotek je potrebno omejiti na razumno mejo, tako da ne onemogoča dela drugih uporabnikov.

Pravila obnašanja na internetu

Za vsak dostop v omrežje internet se lahko vodi evidenca v skladu z informacijsko varnostno politiko, ki je namenjena spremljanju uporabe interneta za statistične prikaze, za planiranje kapacitet strežnikov in za odkrivanje morebitnih zlorab. Ti podatki so tajni in ne vsebujejo osebnih podatkov uporabnikov.

¹ <http://www.arnes.si/pomoc-uporabnikom/pravila-uporabe-omrezja-arnes.html>

Omrežje internet smejo uporabljati le uporabniki informacijskega sistema UM, ki so vključeni v omrežje UM.

Pri vključitvi v omrežje in uporabi storitve ni dovoljeno uporabljati lažnih ali zavajajočih osebnih podatkov.

Nedopustno je pošiljati prispevke za nestrokovne ali osebne polemike, oglase, verižna sporočila ali početi karkoli, kar moti delo drugih uporabnikov.

Ni dovoljeno prenašati podatkov z žaljivo ali pornografsko vsebino, tajnih podatkov ali podatkov, ki so zaščiteni z avtorskimi pravicami ali so v lasti drugih uporabnikov.

Nedopustno je uničevanje ali spreminjanje podatkov, ki so last drugih uporabnikov, ter uporaba programov ali postopkov, ki ovirajo normalno delovanje informacijskih naprav, ki sestavljajo omrežje.

Skrbnik se lahko odloči za ukrepanje v primeru, če bi uporabnik:

- uporabljal javne konferenčne sisteme za komercialno oglaševanje,
- zmerjal, zasmehoval ali žalil druge uporabnike interneta ("flaming"),
- ščuval k verski, rasni, seksualni, nacionalni, politični ali kakšni drugi nestrpnosti,
- izvajal aktivnosti, ki lahko povzročijo pošiljanje velikih količin podatkov in privedejo do zavrnitve storitev (DoS in DDoS napad),
- izvajal aktivnosti, ki lahko privedejo do sprožitve velikega števila zahtev po vzpostavitvi povezav in s tem onemogočijo uporabo storitev drugim uporabnikom ("SYN attack")

V primeru nedovoljene uporabe storitev na omrežju internet, lahko skrbnik začasno onemogoči uporabo sistema za uporabnika.

3. Varnostne zahteve za delovne postaje

3.1 Varnost delovne postaje

Vsak zaposleni je odgovoren in dolžan poskrbeti za varnost in neodtujljivost njemu zaupanih informacijskih sredstev, ki so last podjetja. Uporabnik mora ravnati z delovno postajo na način, ki onemogoča uporabo nepooblaščenih oseb. Na vseh delovnih postajah mora biti:

- med odmori ali odsotnostmi aktivirano zaklepanje tipkovnice in zaslona,
- dokumenti, ki vsebujejo informacije z oznako zaupno, morajo biti šifrirani. Način šifriranja predpiše in uvede RCUM.

Če potujete z zaupnimi informacijami UM na prenosnih medijih (papir, CD, tablica,...), je potrebno informacije zaščititi na enak način kot mobilno napravo.

Opombe:

Gesel, ki niso povezana z uporabniškimi računi (npr. geslo zagon naprave ali šifriranje diska), ni potrebno periodično spreminjati.

Če izgubite ali vam ukradejo mobilno napravo ali zaupne dokumente, je potrebno to takoj sporočiti osebi, odgovorni za ravnanje z informacijsko komunikacijsko tehnologijo.

3.2 Varnost mobilnih naprav

Mobilne naprave (dlančniki, tablice, mobilni telefoni z dostopom do podatkov,...) in prenosni mediji (USB ključ, prenosni diski...) potrebujejo fizično in logično zaščito, če so na njih shranjeni zaupni podatki UM ali se preko naprave do njih dostopa. Potrebno je poskrbeti za naslednje ukrepe:

- uporabnik mora ravnati z mobilno napravo na način, ki onemogoča uporabo nepooblaščenih oseb,
- nastaviti je potrebno zaščitno geslo za vklop in časovno nadzorovan izklop ali zaklepanje na napravah, ki to omogočajo.

Z mobilnimi napravami in prenosnimi mediji je potrebno ravnati varno in skrbno ter jih ni dovoljeno odlagati na nezaščitene in javnih prostorih kjer so izpostavljene pogledom in možnosti odtujitve.

3.3 Zlonamerna programska oprema

Na delovni postaji mora biti nameščena in delujoča protivirusna zaščita. Vrsto in način protivirusne zaščite določa odgovorna oseba za informacijsko varnost. Pri nameščanju protivirusne zaščite lahko pomagajo skrbniki.

Uporabnik mora spoštovati naslednje zahteve:

- ne sme namerno nameščati zlonamerne programske opreme v naprave in jo namerno širiti,
- v primeru suma zlonamerne programske opreme mora o tem takoj obvestiti odgovorno osebo za informacijsko varnost in postopati po njegovih navodilih,
- ne sme odpirati in zaganjati njemu nepoznanih datotek, če ne pozna njihovega izvora,
- zaposleni mora v primeru suma ali ugotovitve, da sistem protivirusne zaščite ne deluje ali ni ustrezno posodobljen, takoj obvestiti lastnika ali odgovorno osebo za informacijsko varnost,

- ne sme preusmerjati obvestil o morebitnih resničnih ali lažnih novih virusih drugim uporabnikom, prijateljem in znancem. Sumljivo pošto mora posredovati skrbniku ali informacijskemu varnostnemu inženirju.

3.4 Požarna pregrada

Na delovni postaji oz. mobilni napravi mora biti nameščena in omogočena požarna pregrada z ustreznimi varnostnimi nastavitvami, če je to tehnično mogoče. Požarna pregrada onemogoča nepooblaščen dostop do podatkov in nedovoljeno uporabo delovne postaje.

3.5 Dostop do delovne postaje

Nepooblaščen in nedogovorjen dostop do datotek na delovni postaji s strani drugih uporabnikov preko računalniškega omrežja podjetja ni dovoljen in je praviloma tudi tehnično onemogočen.

Nepooblaščen in nedogovorjen oddaljen nadzor nad delovnimi postajami ni dovoljen. Pravila za omejeno in kontrolirano uporabo oddaljenega nadzora določa lastnik informacijskega sredstva.

4. Sporočanje varnostnih incidentov

Ob sumu, da se dogaja ali se je zgodil informacijski varnostni incident, je potrebno takoj obvesti odgovorno osebo za informacijsko varnost in se ravnati po posredovanih navodilih.

Zaposleni ne smejo raziskovati ali izvajati akcije proti napadalcu/krivcu. Za obravnavo informacijskih varnostnih incidentov je zadolžena odgovorna oseba za informacijsko varnost.

5. Prehodne in končne določbe

Informacijska varnostna politika za uporabnike velja za vse uporabnike informacijskega sistema UM.

Vsaka kršitev navodil v dokumentu se obravnava kot kršitev delovnih in študijskih obveznosti.

Skrbniki informacijske tehnologije po članicah so dolžni v roku 18 mesecev po sprejemu varnostne politike zagotoviti spoštovanje pravil iz tega dokumenta.

Informacijska varnostna politika za uporabnike prične veljati osmi dan po objavi v Obvestilih Univerze v Mariboru.

Rektor Univerze v Mariboru

Prof. dr. Danijel Rebolj, l.r.