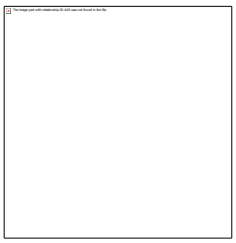

SVEUČILIŠTE U ZAGREBU

MEDICINSKI FAKULTET

SIGURNOSNA POLITIKA

INFORMACIJSKOG SUSTAVA

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeću

1. Odluku o sigurnosti informatičkog sustava

1.1. Ciljevi i opće odredbe

Medicinski fakultet Sveučilišta u Zagrebu prepoznaje važnost i potencijal informatičkih sustava za obrazovanje, razvoj, istraživanje, poslovanje i javne servise. Kao akademska ustanova, MEF dozvoljava širok opseg prava i mogućnosti korištenja informatičkog sustava. S obzirom na sve veći broj sigurnosnih prijetnji na Internetu i informatičkim sustavima, MEF je donio sigurnosnu politiku kojom se reguliraju pravni i opći aspekti vezani uz primjenu i korištenje informatičkih sustava i sustava za upravljanje sigurnošću.

1.2. Opseg

Politika sigurnosti i pripadajući akti primjenjuju se nad svim informatičkim sustavima i njihovim dijelovima uključujući poslužitelje, radne stanice, mrežnu infrastrukturu, sistemski softver, aplikativni softver i podatke koji su u vlasništvu MEF-a ili koje MEF koristi.

1.3. Odgovornost za provedbu politike sigurnosti informatičkog sustava

Posebnim pravilima će se utvrditi struktura odgovornosti za donošenje i provođenje svih sigurnosnih politika, preporuka i pravila.

1.4. Obveza pridržavanja

Obvezu pridržavanja odredaba sigurnosne politike, propisa CARNet-a, akata o sigurnosti i procedura imaju svi korisnici informatičkog sustava MEF-a, uključujući sve zaposlenike, studente i osobe koje privremeno obavljaju poslove prema ugovoru te svi vanjski suradnici ili partneri MEF-a koji dolaze u doticaj s resursima informatičkog sustava.

Nepridržavanje odredaba sigurnosne politike, akata o sigurnosti, procedura i normi od strane zaposlenika MEF-a smatra se povredom radne obaveze, za koju se može dati otkaz uvjetovan skrivljenim ponašanjem zaposlenika te će se utvrditi odgovornost radnika za svaki pojedinačni slučaj nepridržavanja bilo koje od uputa ili odredbi ovog dokumenta i akata koji će biti doneseni na temelju njega.

Nepridržavanje odredaba sigurnosne politike, akata o sigurnosti, procedura i normi od strane vanjskih korisnika, suradnika i partnera smatra se povredom ugovornih obaveza te je razlog za izvanredni raskid ugovora.

Nepridržavanje odredaba sigurnosne politike, akata o sigurnosti, procedura i normi od strane studenata smatra se prekršajem te je razlog za uskraćivanje budućeg korištenja informatičkih resursa i pokretanje stegovnog postupka.

1.5. Prateći dokumenti

Ova odluka predstavlja krovni dokument sigurnosne politike MEF-a. Uz ovu odluku, MEF će primjenjivati niz dokumenata koji određuju sigurnosne politike, pravila i procedure za pojedine dijelove ili resurse informatičkog sustava. Svi ti akti imaju jednaku pravnu važnost.

Prateći dokumenti će se donositi po potrebi, a usvojeni akti podložni su revizijama.

1.6. Provjere i revizije

Sigurnosna politika i svi uključeni akti podložni su provjerama i revizijama. Provjere će pratiti efikasnost sigurnosne politike u slučaju sigurnosnih incidenata. Na osnovi rezultata tih provjera, radit će se, po potrebi i po odluci dekana, revizije sigurnosne politike. Revizije se mogu raditi i u slučaju promjena na informatičkom sustavu, novih prijetnji, promjena u procjeni rizika i drugih događaja koji mogu utjecati na sigurnost informatičkog sustava.

Provodit će se i periodičke provjere i revizije, koje uključuju:

1. provjeru i procjenu efikasnosti sigurnosne politike,
2. procjenu troškova i utjecaja na efikasnost poslovanja,
3. ocjenu utjecaja tehnoloških promjena na sigurnosnu politiku i sigurnost.

Za provjere i revizije sustava sigurnosti odgovoran je Voditelj sigurnosti.

1.7. Stupanje na snagu

Ova Odluka stupa na snagu i primjenjuje se danom objave na oglasnoj ploči Medicinskog fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

2. Pravila o odgovornosti za sigurnost

2.1. Ciljevi i opće odredbe

Cilj ovih Pravila je uspostavljanje sustava odgovornosti za provođenje i nadzor sustava za upravljanje sigurnošću na MEF-u.

2.2. Opseg

Ova pravila odnose se na sustav za upravljanje sigurnošću MEF-a.

2.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti MEF-a, kojega imenuje dekan.

2.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju sve osobe odgovorne za sigurnost te korisnici računalno – komunikacijskog sustava MEF-a.

2.5. Raspodjela odgovornosti

Dekan MEF-a donosi i potpisuje sigurnosnu politiku.

Dekan osniva Savjet za sigurnost i imenuje njegove članove. Savjet za sigurnost je tijelo koje je odgovorno za implementaciju i funkcioniranje sustava za upravljanje sigurnošću. Ono predlaže dekanu usvajanje sigurnosnih politika, pravila, imenovanja odgovornih osoba i druge odluke od strateške važnosti za sigurnost računalno – komunikacijskog sustava MEF-a.

Savjet za sigurnost mora imati najmanje pet članova. Jedan je iz sastava Dekanskog kolegija fakulteta, a drugi je Voditelj sigurnosti treći je Sistem inženjer i CARNet koordinator. U Savjetu može biti i osoba koja nije zaposlenik MEF-a.

Savjet za sigurnost će se sastajati po potrebi, ali i periodički, najmanje jednom u svakih šest mjeseci.

Dekan imenuje i Voditelja sigurnosti. On je glavni operativac za sve poslove vezane uz sustav za upravljanje sigurnošću. Voditelj sigurnosti može samostalno donositi sve odluke vezane za sigurnost. On je jedan od članova Savjeta za sigurnost. Na periodičkim ili izvanrednim sastancima Savjeta za sigurnost, Voditelj sigurnosti podnosi izvještaj i obavještava o svim bitnim događajima vezanim uz sigurnost. Voditelj sigurnosti dužan je provoditi odluke dekana i Savjeta za sigurnost.

Voditelj sigurnosti može imenovati svog pomoćnika, koji onda ima iste ovlasti kao i Voditelj sigurnosti, a za svoj rad odgovoran je Voditelju. Voditelj sigurnosti može imenovati administratore za sigurnost, koji onda imaju ovlasti nad dodijeljenim im sustavima, resursima, pravilnicima ili procedurama. Oni su za svoj rad odgovorni Voditelju sigurnosti, a on može u svakom trenutku povući svoja imenovanja.

Svaki resurs treba imati vlasnika ili administratora, odnosno odgovornu osobu za njegovu sigurnost. Ta osoba može delegirati poslove nekom drugom, ali odgovornost za dodijeljeni resurs ostaje na odgovornoj osobi.

Informatički odsjek i osoblje zaduženo za informatiku također su odgovorni za sigurnost računalno – komunikacijskog sustava. Oni moraju surađivati s osobljem za sigurnost i izvještavati ih o uočenim potencijalnim sigurnosnim problemima.

2.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

2.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

3. Pravila o korištenju opreme

3.1. Ciljevi i opće odredbe

Cilj Pravila o korištenju opreme je određivanje načina na koje je dopušteno koristiti informatičku opremu Medicinskog fakulteta u Zagrebu.

3.2. Opseg

Ova pravila odnose se na svu računalnu (uključujući programe) i komunikacijsku opremu u vlasništvu MEF-a.

3.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

3.4. Obveza pridržavanja

Obvezu pridržavanja ovih Pravila imaju sve fizičke i pravne osobe koje koriste navedenu opremu, što uključuje i:

- zaposlenike MEF-a,
- studente,
- udruge,
- vanjske tvrtke i partnere,
- goste.

Nepridržavanje odredaba sigurnosne politike, akata o sigurnosti, procedura i normi od strane zaposlenika MEF-a smatra se povredom radne obaveze, za koju se može dati otkaz uvjetovan skrivljenim ponašanjem zaposlenika te će se utvrditi odgovornost radnika za svaki pojedinačni slučaj nepridržavanja bilo koje od uputa ili odredbe ovih akta i akata koji će biti doneseni na temelju njega.

Nepridržavanje odredaba sigurnosne politike, akata o sigurnosti, procedura i normi od strane vanjskih korisnika, suradnika i partnera smatra se povredom ugovornih obaveza te je razlog za izvanredni raskid ugovora.

Nepridržavanje odredaba sigurnosne politike, akata o sigurnosti, procedura i normi od strane studenata smatra se prekršajem te je razlog za uskraćivanje budućeg korištenja informatičkih resursa i pokretanje stegovnog postupka.

3.5. Pravila korištenja

Sva oprema, nabavljena ili unajmljena od strane MEF-a, pripada MEF-u, a korisnicima se daje na korištenje radi obavljanja posla. Svi sadržaji na korištenoj opremi također su u vlasništvu MEF-a, ukoliko nije posebnim dokumentom (pravila, ugovor, odluka…) drugačije određeno i izuzev autorskih radova korisnika računalno – komunikacijskog sustava MEF-a.

MEF zadržava pravo nadzora nad načinom korištenja opreme, kako je definirano u Pravilima o nadgledanju i nadzoru informatičkih resursa.

Svi korisnici mogu koristiti samo opremu koja im je dodijeljena na korištenje od strane odgovornih osoba MEF-a, odnosno Odsjeka za informatiku.

Za korištenje vlastite ili neke treće opreme potrebna je suglasnost odgovornih osoba MEF-a (osoblje za sigurnost i Informatički odsjek) i za tu opremu važe, za vrijeme korištenja na MEF-u, sva pravila kao i za opremu u vlasništvu MEF-a.

Na MEF-u može biti locirana i oprema koja nije u vlasništvu MEF-a (npr. CARNet-ova oprema, oprema drugih pružatelja usluga…). Za tu opremu važe pravila korištenja prema Ugovoru s trećim stranama, koji se potpisuje s takvim partnerima.

Nedozvoljenim se smatra svako korištenje opreme na način koji bi doveo do povrede važećih zakona ili drugih propisa ili pravila MEF-a ili etičkih normi ili bi mogao izazvati materijalnu ili nematerijalnu štetu za MEF.

Nedozvoljena korištenja uključuju i slijedeće radnje:

- povreda prava i privatnosti drugih ljudi te intelektualnog vlasništva,
- uvrede, ponižavanje, širenje mržnje, netrpeljivosti, vrijeđanje po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti,
- namjerno generiranje ili prosljeđivanje malicioznih programa (virusi, crvi, trojanci…),
- neovlašteno skeniranje portova i prisluškivanje prometa,
- generiranje velike količine prometa s ciljem uskraćivanja resursa korisnicima ili pokušaji onesposobljavanja računala, programa i komunikacijske mreže na bilo koji drugi način,
- korištenje nelegalnih kopija programa,
- korištenje programa na način koji nije u skladu s dobivenom ili prihvaćenom licencom,
- korištenje nedozvoljenih programa (Voditelj sigurnosti ima pravo zabraniti neke programe za korištenje, a uvid u tu listu mora biti osiguran svim korisnicima),
- razmjena autorski zaštićenih materijala bez suglasnosti vlasnika prava, odnosno bez plaćanja propisane naknade,
- neovlašteno kopiranje materijala zaštićenih *copyright*-om,
- preuzimanje tuđeg identiteta,
- provođenje bilo kakvih napada na vanjska računala, poslužitelje ili mreže,
- slanje masovnih poruka komercijalne ili nekomercijalne prirode (*spam*, *hoax*, lanci sreće…),
- neovlašteno korištenje opreme u komercijalne svrhe (npr. Web *hosting*),
- otvaranje poslužiteljskih servisa (npr. Mail, Web, FTP) bez suglasnosti Voditelja sigurnosti ili Administratora za sigurnost,

- pokušaj pristupa zaštićenim informacijama za koje korisnik nije autoriziran,
- sve druge radnje kojima se povređuju odredbe ovih Pravila…

Za pojedine grupe korisnika MEF može donijeti posebna pravila ili postupke kojima će detaljnije definirati pravila prihvatljivog korištenja opreme za te korisnike.

Pojedine organizacijske jedinice unutar MEF-a mogu definirati vlastita pravila korištenja. Oni moraju biti u skladu s ovim Pravilima, ali mogu dodatno i detaljnije definirati pojedine stvari.

Za provedbu ovih Pravila odgovoran je Voditelj sigurnosti. On može dati ovlaštenja jednom ili više Administratora za sigurnost. Oni su odgovorni za provođenje ovog i drugih pravila na računalnoj i komunikacijskoj opremi. Oni daju ovlaštenja pojedinim korisnicima na korištenoj opremi. Pojedinim korisnicima mogu se dati i administratorske ovlasti, koje izdaje administrator, a on ih može i povući. Korisnik ne smije na opremi koju koristi raditi ništa što bi negativno utjecalo na provođenje ovog i drugih pravila niti instalirati sistemske aplikacije bez odobrenja administratora. Administratori pri tome moraju, u najvećoj mogućoj mjeri, a koja ne ugrožava sigurnost opreme, sustava ili drugih korisnika, poštovati privatnost korisnika i podataka na opremi koju korisnik koristi.

MEF može zabraniti ili ograničiti upotrebu nekih programa ili servisa ukoliko postoje sigurnosni razlozi za to (npr. ukoliko se distribuiraju nelegalni ili nelicencirani sadržaji, MEF može zabraniti ili ograničiti upotrebu *peer-to-peer* aplikacija i servisa).

MEF zadržava pravo iznimne zabrane ili ograničavanja pristupa pojedinim sadržajima na Internetu na onim računalima gdje bi taj sadržaj mogao ugroziti radni proces. Odluku o tome, koja mora sadržavati što se zabranjuje i razloge za to, mora usvojiti Fakultetsko vijeće na prijedlog Savjeta za sigurnost i Dekana.

3.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

3.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

4. Pravila o kontroli pristupa informatičkim resursima

4.1. Ciljevi i opće odredbe

Sve osjetljive i povjerljive informacije i informatičke resurse potrebno je zaštiti od neovlaštenog pristupa, čitanja i korištenja.

4.2. Opseg

Ova pravila odnose se na zaštitu na razini pojedinih resursa, a obuhvaćaju računalno – komunikacijski sustav MEF-a.

4.3. Odgovornost za provedbu

Ovaj dokument usvojen je od strane dekana MEF-a. Za njegove provedbu odgovoran je Voditelj sigurnosti, imenovan od strane dekana.

4.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju osobe odgovorne za sigurnost na MEF-u, sistemski administratori te svi korisnici računalno – komunikacijskog sustava MEF-a.

4.5. Pristup operacijskom sustavu i administriranje računala

Odsjek za informatiku i ovlašteni sistemski administratori odgovorni su za administriranje računalne i mrežne opreme. Svaki informatički resurs (računalo, uređaj, servis, aplikacija…) mora imati imenovanog administratora. Voditelj sigurnosti i administratori za sigurnost odgovorni su za sigurnost resursa. Informatičko i osoblje za sigurnost mora usko surađivati, a Voditelj sigurnosti ima pravo zatražiti potrebne radnje i ovlasti od informatičkog osoblja, koje su mu ovi dužni provesti ili omogućiti. U slučaju konflikta oko ovlasti, slučaj se predaje na razmatranje Savjetu za sigurnost.

Svako računalo mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju operacijskog sustava i programa. Ukoliko neki korisnici žele sami administrirati osobno računalo koje koriste, moraju podnijeti zahtjev Odsjeku za informatiku, a zahtjev mora odobriti Savjet za sigurnost. Informatičko osoblje ili Savjet za sigurnost mogu u bilo kojem trenutku privremeno povući to odobrenje uz pismeno obrazloženje.

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se spriječile nedopuštene aktivnosti.

Korisnici moraju opremu koristiti u skladu s Pravilima o korištenju opreme. Moraju dopustiti informatičkom osoblju i osoblju zaduženom za sigurnost pristup i intervencije na svom računalu ili promijeniti konfiguraciju i druge parametre u skladu s njihovim zahtjevima.

Informatičko osoblje i osoblje za sigurnost dužno je u svome radu poštovati privatnost korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla. Svaka zlouporaba ovlasti strogo je zabranjena.

Korisnici mogu osigurati zaštitu privatnih ili autorskih informacija kriptiranjem istih, kako je navedeno ovim Pravilima.

4.6. Zaštita osjetljivih podataka

Osim kontrola pristupa na nivou računalne mreže, osjetljive i povjerljive podatke u elektroničkom obliku potrebno je dodatno zaštiti prilikom spremanja na tvrde diskove. Postoje najmanje dvije kategorije podataka koje treba zaštiti:

- službeni podaci (npr. medicinskog ili etičkog sadržaja) za koje MEF odredi da se moraju zaštiti,
- privatni ili autorski podaci koje korisnik želi zaštiti.

MEF će izraditi klasifikaciju i popis službenih podataka i informacija koje se moraju zaštiti.

Korisnici imaju pravo zaštiti podatke koji su u njihovom vlasništvu ili na koje imaju autorska ili druga prava.

Za zaštitu je preporučljivo koristiti spremanje i čuvanje podataka na tvrdim diskovima u kriptiranom obliku uz korištenje odgovarajućih enkripcijskih algoritama i ključeva.

Ovakav način zaštite potrebno je primjenjivati prvenstveno na tvrde diskove (zbog mogućnosti neovlaštenog čitanja prilikom popravka ili servisa), a po potrebi, mogu se koristiti i za druge medije za pohranu podataka.

4.7. Pristup aplikacijama i poslužiteljima

Pristup se može kontrolirati i na nivou pojedine aplikacije, servisa ili poslužitelja. Svaki od navedenih resursa mora imati svog vlasnika ili administratora, koji je odgovoran za odabir i provedbu metode kontrole pristupa, u suglasnosti s Voditeljem sigurnosti ili pomoćnikom.

4.8. Pristup računalnoj mreži

MEF može kontrolirati pristup informatičkim resursima i na razini pristupa računalnoj mreži. Korisnici koji nisu zaposlenici fakulteta ne smiju samovoljno priključivati na mrežu računala i druge uređaje, već uz suglasnost i prema uputama Odsjeka za informatiku i osoblja za sigurnost.

4.9. Korištenje prijenosnih uređaja i medija

Za pristup prijenosnih uređaja koji nisu vlasništvo fakulteta (prijenosna računala, ručni uređaji…) računalno – komunikacijskom sustavu MEF-a potrebna je suglasnost Voditelja sigurnosti ili njegovog pomoćnika.

Dozvoljeno je korištenje prijenosnih medija za pohranu podataka (npr. prijenosni tvrdi diskovi), ali korisnici moraju voditi računa o njihovoj zaštiti dok se koriste van računalno – komunikacijskog sustava MEF-a.

Također, potrebno je voditi posebnu pažnju o zaštiti osjetljivih podataka na prijenosnim računalima i medijima kada se nalaze van MEF-a. To uključuje fizičku zaštitu, kontrolu pristupa, kriptiranje osjetljivih podataka…

U slučaju incidentne situacije kojoj je uzrok jedno računalo Savjet za sigurnost ima pravo privremeno isključiti korisnika iz mreže uz objašnjenje.

4.10. Nadgledanje i nadzor informatičkih resursa

MEF ima pravo, po nalogu i pod odgovornošću Savjeta za sigurnost, provoditi, po potrebi ili periodički, nadgledanje i nadzor informatičkih resursa, uključujući mrežnu komunikaciju, osobna računala, poslužitelje, servise, aplikacije…

Pri tome je osoblje koje provodi nadzor dužno poštovati privatnost korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla. Svaka zlouporaba ovlasti strogo je zabranjena.

Korisnici mogu osigurati zaštitu privatnih ili autorskih informacija kriptiranjem istih, kako je navedeno ovim Pravilima.

4.11. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

4.12. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

5. Pravila o internoj sigurnosti

5.1. Ciljevi i opće odredbe

Cilj ovih Pravila je reguliranje zaštite pojedinih dijelova mreže Medicinskog fakulteta u Zagrebu (u daljnjem tekstu: MEF) od internih napada s drugih dijelova iste mreže.

5.2. Opseg

Ova Pravila odnose se na računalno – komunikacijski sustav MEF-a.

5.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

5.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju svi administratori i korisnici računalno – komunikacijskog sustava MEF-a.

5.5. Interna zaštita

S obzirom na brojnost i heterogenost korisnika računalno – komunikacijskog sustava MEF-a te na činjenicu da velik dio napada u svijetu dolazi s internih mreža, potrebno je poduzeti i mjere zaštite pojedinih grupa korisnika od drugih korisnika s interne mreže.

MEF će napraviti podjelu i grupiranje korisnika te će za svaku grupu biti implementirana odgovarajuća sigurnosna pravila. U pravilu, grupama s višim sigurnosnim rizikom treba biti zabranjen pristup s ostatka mreže. Pri tome treba voditi računa da se što manje ugrožava dostupnost mrežnih i Internet servisa i mogućnost komuniciranja.

Grupiranje i organizacija mreže treba slijediti organizacijsku strukturu MEF-a. Svaka organizacijska cjelina ima pravo na zaštitu i kontrolu prometa. Oni mogu sami definirati zahtjeve, koji moraju biti u skladu s ovom sigurnosnom politikom, a treba ih odobriti Savjet za sigurnost.

Korisnicima je zabranjeno samovoljno mijenjati pripadnost dodijeljenoj grupi.

5.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

5.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

6. Pravila o udaljenim lokacijama

6.1. Ciljevi i opće odredbe

Cilj Pravila o udaljenim lokacijama je reguliranje sigurnosnih pitanja prilikom povezivanja udaljenih lokacija MEF-a na računalno – komunikacijski sustav.

6.2. Opseg

Ova pravila odnose se na računalno – komunikacijski sustav MEF-a, uključujući udaljene lokacije.

6.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

6.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju osobe odgovorne za sigurnost na MEF-u i administratori.

6.5. Povezivanje udaljenih lokacija

Udaljene lokacije su sve lokacije koje pripadaju MEF-u i koje se smatraju dijelom računalno – komunikacijskog sustava MEF-a, a ne nalaze se na glavnoj lokaciji.

Za udaljene lokacije vrijede sva pravila i sigurnosne politike usvojene za MEF.

Kako udaljene lokacije u praksi često služe kao infrastruktura za napade na središnji dio sustava, potrebno je posebnu pažnju posvetiti kontroli provođenja sustava za upravljanje sigurnošću na udaljenim lokacijama.

MEF će omogućiti udaljenim lokacijama pristup računalno - komunikacijskom sustavu ili njegovim dijelovima.

Za sav promet između udaljene lokacije i interne mreže MEF-a mora biti osigurana autentičnost, povjerljivost i integritet podataka.

Autentičnost znači da se točno zna od koga dolaze podaci.

Povjerljivost znači da su podaci zaštićeni od neovlaštenog čitanja na putu između udaljenog korisnika do mreže MEF-a.

Integritet podataka znači da je osigurano da podaci nisu izmijenjeni na putu između udaljenog korisnika do mreže MEF-a.

Zabranjeno je instaliranje modema i drugih uređaja za udaljeni pristup na udaljenim lokacijama bez pismenog odobrenja Voditelja sigurnosti MEF-a.

Ukoliko udaljena lokacija ostvaruje izravni pristup središnjem računalno – komunikacijskom sustavu MEF-a, ona može ostvariti samostalnu vezu na Internet samo uz pismenu dozvolu Voditelja sigurnosti i uz sve mjere zaštite definirane ovim Pravilima i drugim relevantnim dokumentima i uputama od strane odgovornih osoba MEF-a.

6.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

6.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

7. Pravila o udaljenim korisnicima

7.1. Ciljevi i opće odredbe

Cilj Pravila o udaljenim korisnicima je određivanje načina na koji je moguće ostvariti i regulirati pristup udaljenih korisnika.

7.2. Opseg

Ova pravila odnose se na sve korisnike računalno – komunikacijskog sustava MEF-a koji pristupaju internim resursima izvana.

7.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

7.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju sve fizičke i pravne osobe koje pristupaju internoj mreži MEF-a s udaljenih lokacija, što uključuje pristup od kuće, s puta ili druge vanjske lokacije.

7.5. Pristup udaljenih korisnika

Pravo pristupa internom dijelu računalno – komunikacijskog sustava MEF-a mora odobriti Voditelj sigurnosti MEF-a.

MEF zadržava pravo udaljeni pristup ograničiti na pojedine resurse.

Udaljeni korisnik dužan je pridržavati se uputa odgovornih osoba MEF-a i udaljeni pristup koristiti isključivu u obimu i namjeni koji su mu odobreni.

Za sav promet između udaljenog korisnika i interne mreže MEF-a, mora biti osigurana autentičnost, povjerljivost i integritet podataka.

Autentičnost znači da se točno zna od koga dolaze podaci.

Povjerljivost znači da su podaci zaštićeni od neovlaštenog čitanja na putu između udaljenog korisnika do mreže MEF-a.

Integritet podataka znači da je osigurano da podaci nisu izmijenjeni na putu između udaljenog korisnika i mreže MEF-a.

Zabranjeno je instalirati i koristiti modeme, VPN poslužitelje ili druge načine udaljenog pristupa na mreži MEF-a bez odobrenja Voditelja sigurnosti.

Udaljeni korisnici odgovorni su za onemogućavanje korištenja prava udaljenog pristupa od strane neautoriziranih osoba (uključujući rodbinu, prijatelje…). Autentikacijski podaci ne smiju se dijeliti s drugim osobama.

Udaljeni korisnici moraju se pridržavati svih važećih pravila o sigurnosti MEF-a, uključujući:

- računala moraju imati instaliran i osvježavan antivirusni program,
- računala moraju imati instalirane najnovije zakrpe operacijskog sustava i programa,
- prilikom spajanja na Internet, treba koristiti osobni vatrozid.

Zabranjeno je istovremeno korištenje otvorene veze prema Internetu i veze na internu mrežu MEF-a (*VPN split tunneling*, korištenje više Internet veza i sl.).

Udaljeni korisnici moraju voditi računa o zaštiti povjerljivih dokumenata i sadržaja na udaljenom računalu jednako kao na računalima koja se nalaze na mreži MEF-a.

7.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

7.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

8. Pravila o trećim stranama

8.1. Ciljevi i opće odredbe

Cilj ovih Pravila je reguliranje sigurnosnih pitanja prilikom povezivanja udaljenih lokacija MEF-a na računalno – komunikacijski sustav.

8.2. Opseg

Ova Pravila odnose se na računalno – komunikacijski sustav MEF-a.

8.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

8.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju osobe odgovorne za sigurnost na MEF-u, informatički administratori, pravna služba MEF-a te vanjske fizičke i pravne osobe koje pristupaju računalno – komunikacijskom sustavu MEF-a.

8.5. Pristup trećih strana informatičkim resursima

Ukoliko poslovne potrebe to nalažu, moguće je osigurati pristup trećih strana, fizičkih i pravnih osoba, informatičkim resursima MEF-a. Omogućavanjem takovog pristupa može doći ne samo do gubitka povjerljivosti informacija, već i do narušavanja njihovog integriteta i raspoloživosti. Slučajnim ili namjernim otkrivanjem informacija te njihovom modifikacijom moguće je narušiti poslovni kredibilitet i/ili uzrokovati direktne financijske štete za MEF.

Zbog tih razloga potrebno je ugovorom koji treća strana potpisuje definirati sigurnosne kontrole i pravila kojih se treća strana mora pridržavati.

Pristup trećih strana odnosi se na oboje – fizički pristup i logički pristup.

Pojam treće strane odnosi se na sve pravne i fizičke osobe koje zbog bilo kakvih potreba pristupaju informatičkim resursima MEF-a, a koje uključuju i sljedeće:

- programsku i/ili sklopovsku potporu i održavanje, gdje je potrebno osigurati pristup na razini sustava i/ili aplikacije,
- poslovne partnere, gdje je potrebno osigurati mehanizme za pristup i razmjenu informacija i/ili baza podataka,
- konzultante, gdje je potrebno omogućiti pristup raznim informacijskim resursima tvrtke,
- servisno osoblje i privremene zaposlenike.

Pristup trećih strana informatičkim resursima MEF-a potrebno je ograničiti samo na one resurse kojima je taj pristup nužan. Ukoliko postoji potreba za takovim pristupom, potrebno je provesti odgovarajuću procjenu rizika, uočiti sigurnosne implikacije, te definirati odgovarajuće sigurnosne kontrole. Prava pristupa i kontrole trebaju biti definirani i dogovoreni ugovorom.

8.6. Gosti MEF-a

Posebna kategorija su gosti MEF-a (vanjski predavači, povremeni suradnici, posjetitelji…). Oni pristupaju računalno – komunikacijskom sustavu MEF-a povremeno i privremeno te ne moraju imati ugovor. Osim toga, za njih vrijede sva pravila pristupa kao za treće strane.

Gosti se ne smiju samovoljno priključivati na mrežu MEF-a, već je za to odgovoran Informatički odsjek MEF-a. MEF može prije priključivanja provjeriti sigurnost ili zahtijevati od gosta dokaze o sigurnosti gostujućeg računala te sugerirati i provesti potrebne mjere za podizanje razine sigurnosti.

Gostujuća računala trebaju biti smještena u posebne zone unutar mreže MEF-a sa strogo ograničenim i kontroliranim pravima pristupa internim računalno – komunikacijskim resursima MEF-a.

8.7. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

8.8. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

9. Pravila o povezivanju na Internet

9.1. Ciljevi i opće odredbe

Cilj Pravila o povezivanju na Internet je reguliranje zaštite računalno – komunikacijskih resursa MEF-a i korisnika od sigurnosnih prijetnji koje mogu doći s Interneta.

9.2. Opseg

Ova pravila odnose se na računalno – komunikacijski sustav MEF-a.

9.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

9.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju svi administratori i korisnici računalno – komunikacijskog sustava MEF-a.

9.5. Zaštita od Interneta

Računalnu mrežu MEF-a potrebno je podijeliti na javni dio (demilitarizirana zona – DMZ) i interni dio. DMZ je otvoren prema Internetu, na njemu se nalaze servisi dostupni s Interneta.

Internom dijelu u pravilu treba biti zabranjen svaki izravni pristup s Interneta, osim u slučajevima, za kakve je potrebno odobrenje Savjeta za sigurnost. Na internom dijelu će se nalaziti sva računala MEF-a, osim onih sa servisima kojima je potreban izravni pristup s Interneta.

Internim računalima treba biti omogućen pristup Internetu u najvećoj mjeri koja ne ugrožava sigurnost mreže MEF-a. MEF može posebnim odredbama i odlukama drugačije regulirati dostupnost s Interneta i prava pristupa Internetu s pojedinih dijelova mreže ili računala.

Unutar javnog dijela mreže (DMZ), moguće je formirati više zona s različitim pravilima komunikacije i pristupa s Interneta. Pristup računalima i servisima u DMZ-u također je potrebno ograničiti samo na javno dostupne servise te nadzirati i kontrolirati. Posebno treba osigurati da računala u DMZ-u uvijek imaju instalirane najnovije sigurnosne zakrpe operacijskih sustava i drugih aplikacija.

Za informacije koje se objavljuju na javno dostupnim sustavima, a nisu klasificirane kao potpuno javne (dostupne svima), nužno je osigurati odgovarajuće metode autentikacije, te, po potrebi, dodatne oblike zaštite.

Strogo je zabranjeno korištenje Interneta i računalno – komunikacijskog sustava MEF-a za nabavljanje i distribuciju nelegalnog sadržaja, uključujući sadržaja na kojem postoje autorska prava.

9.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

9.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

10. Pravila o zaštiti od virusa i malicioznih programa

10.1. Ciljevi i opće odredbe

Cilj Pravila o zaštiti od virusa i malicioznih programa je zaštita računalnih resursa MEF-a od virusa i sličnih malicioznih programa (crvi, trojanski programi, logičke bombe, *spyware* i *adware* programi…).

10.2. Opseg

Ova Pravila odnose se na svu računalnu opremu MEF-a.

10.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

10.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju svi administratori i korisnici računalno – komunikacijskog sustava MEF-a.

10.5. Zaštita od virusa i malicioznih programa

Anti-virusnu zaštitu potrebno je provoditi u najvećoj mogućoj mjeri, i to na više razina:

- na svim osobnim računalima,
- na svim poslužiteljima,
- na poslužiteljima elektroničke pošte potrebno je kontrolirati svu dolaznu i odlaznu elektroničku poštu.

MEF zadržava pravo propisati dodatne procedure za zaštitu od virusa i malicioznih programa.

Anti-virusni programi moraju se redovito održavati i osvježavati bazu uzoraka virusa.

Za instaliranje i održavanje anti-virusnih programa odgovorni su sistemski administratori i osoblje za sigurnost MEF-a. Korisnici ne smiju samovoljno isključiti anti-virusnu zaštitu na svome računalu.

MEF može, po potrebi, definirati posebne procedure za zaštitu od drugih tipova malicioznih programa (crvi, trojanski programi, logičke bombe, *spyware* i *adware* programi…).

10.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

10.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

11. Pravila o zaštiti od *spama*

11.1. Ciljevi i opće odredbe

Cilj Pravila o zaštiti od spama je reguliranje zaštite korisnika elektroničke pošte na MEF-u od neželjenih poruka (engl. *spam*).

11.2. Opseg

Ova Pravila odnose se na sustav elektroničke pošte na MEF-u.

11.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

11.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju svi administratori sustava elektroničke pošte na MEF-u.

11.5. Zaštita od *spama*

Neželjene poruke elektroničke pošte potrebno je detektirati i tretirati na jedan od slijedećih načina:

- detektirane i označene *spam* poruke proslijediti primaocu, koji ih na osnovi oznake može tretirati drugačije od regularnih poruka,
- detektirane i označene *spam* poruke staviti u karantetnu i ne proslijediti ih primaocu.

Administratori moraju nadzirati rad anti-spam sustava i prilagođavati ga na način da broj lažnih detekcija, posebno lažnih pozitivnih, bude minimalan.

Korisnicima računalno – komunikacijskog sustava MEF-a strogo je zabranjeno generiranje i slanje te prosljeđivanje *spama*.

11.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

11.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

12. Pravila o fizičkoj sigurnosti i sigurnosti opreme

12.1. Ciljevi i opće odredbe

Cilj Pravila o fizičkoj sigurnosti je određivanje minimalnih zahtjeva za osiguranje fizičke zaštite osjetljivih računalno – komunikacijskih resursa Medicinskog fakulteta u Zagrebu (u daljnjem tekstu: MEF).

12.2. Opseg

Ova pravila odnose se na računalnu i komunikacijsku opremu MEF-a.

12.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

12.4. Obveza pridržavanja

Obvezu pridržavanja ovih Pravila imaju osobe odgovorne za sigurnost na MEF-u, administratori računalnih sustava te korisnici računalno – komunikacijskog sustava MEF-a.

12.5. Sigurne zone

Unutar prostora MEF-a potrebno je definirati sigurne zone. Pristup sigurnim zonama mora biti kontroliran na način da je ulaz omogućen samo autoriziranim osobama. Neovlašteni pristup treba biti strogo onemogućen, između ostalog, fizičkim onemogućavanjem pristupa (čvrsti zidovi i prozori koji potpuno ograđuju prostor osim na predviđenim ulazima i požarnim vatima, alarmni sustavi, kontrolirani ulaz, alarmirana požarna vrata s automatskim zatvaranjem i sl.). Moguće je definirati više razina sigurnih zona za zaštitu informatičkih resursa i povjerljivih dokumenata (npr. Zaštićena zona i Posebno zaštićena zona). Posebnim aktima definirat će se područja koja spadaju u te zone, tko je odgovoran za njihovu kontrolu te tko ima pravo pristupa.

Računalna i komunikacijska oprema koja obavlja kritične funkcije ili sadrži osjetljive podatke fizički se odvaja u sigurne zone. Preporučljivo je da se u posebno zaštićene zone ulazi samo po potrebi (intervencije, servisiranje opreme…), dakle da se administratorima osigura radni prostor odvojeno od prostorija u kojima je smještena kritična oprema.

Unutar sigurnih zona mogu postojati prostori, sobe, ormari ili sefovi sa zasebnom politikom pristupa, koji mogu biti zaključani i/ili na drugi način zaštićeni. Ovakvi prostori ne bi trebali biti na javno dostupnim i prometnim mjestima.

12.6. Sigurnost opreme

Potrebno je osigurati zaštitu opreme od gubitka, oštećenja i neovlaštenog korištenja te minimizirati rizik od prekida poslovnog procesa. Oprema mora biti smještena i zaštićena tako da se minimizira rizik od neautoriziranog pristupa i štetnih utjecaja okoline:

- oprema treba biti smještena tako da se minimizira nepotrebni pristup u radne zone,
- informatička oprema koja obrađuje ili sadržava osjetljive podatke mora biti smještena tako da njena vizualna sučelja nisu izložena pogledima,
- posebno osjetljiva oprema (oprema bitna za poslovanje i funkcioniranje računalno – komunikacijskog sustava) mora biti izolirana i posebno zaštićena,
- potrebno je voditi računa o minimiziranju rizika od krađe, vatre, eksploziva, dima, vode, prašine, vibracija, kemijskih čimbenika, električne energije i elektromagnetskog zračenja,
- u prostorijama s informatičkom opremom zabranjeno je konzumiranje hrane, pića i pušenje,
- potrebno je osigurati odgovarajuće temperaturne uvjete u prostorijama za svu opremu,
- prilikom smještanja osjetljive opreme treba voditi računa o potencijalnom utjecaju opasnosti u susjedstvu (npr. požar u susjednim prostorijama ili curenje vode kroz krov zgrade).

Oprema treba biti zaštićena od prekida u opskrbi strujom i drugih električnih anomalija. Električno napajanje mora u potpunosti odgovarati specifikacijama proizvođača opreme.

Za osjetljivu opremu mora se osigurati neprekinuto napajanje električnom energijom barem neko vrijeme nakon nestanka struje. To se može postići UPS uređajima. Ukoliko neka oprema mora raditi dulje vrijeme u slučaju nestanka struje, potrebno je osigurati rezervni generator.

Električni i telekomunikacijski kablovi moraju biti zaštićeni od presretanja ili oštećenja:

- mrežni kabeli ne bi trebali prolaziti javnim i lako dostupnim područjima,
- električni i komunikacijski kabeli trebaju biti razdvojeni kako bi se izbjegla interferencija.

Osjetljivi i kritični sustavi trebaju imati posebne mjere zaštite:

- korištenje oklopljenih kablova i zaključanih soba ili kutija na krajnjim i drugim dostupnim točkama,
- korištenje svjetlovodnih kablova,
- potrebno je redovito aktivno pretraživanje neautoriziranih uređaja priključenih na kablovski sustav.

Opremu treba pravilno održavati (prema uputama proizvođača) kako bi se postigao dugačak i ispravan rad.

Jednake ili odgovarajuće mjere sigurnosti i zaštite moraju se primjenjivati za opremu koja se koristi na svim lokacijama MEF-a, kao i na lokacijama koje nisu u vlasništvu MEF-a (vanjske lokacije). Posebnu pažnju treba obratiti na zaštitu opreme na javnim mjestima (ne ostavljati opremu bez kontrole na javnim mjestima, nositi je kao ručnu prtljagu prilikom putovanja itd.).

Oprema koja sadrži osjetljive podatke treba prije deponiranja biti fizički uništena ili podaci moraju biti na siguran način izbrisani. Sva oprema koja sadrži jedinice za pohranu

podataka mora biti provjerena prije odlaganja, kao i oštećena oprema i oštećene jedinice za pohranu podataka.

12.7. Općenite sigurnosne mjere

U cilju zaštite svih informacija i sustava za njihovu obradu, potrebno je primjenjivati pravila kojima će se sigurnosni rizik od neovlaštenog pristupa, uništenja, krađe ili gubitka svesti na prihvatljivu razinu. Posebnu je pažnju potrebno posvetiti pravilima sigurnog korištenja i održavanja radnog okruženja korisnika, pogotovo u pogledu nesmotrenog odlaganja povjerljivih dokumenata i digitalnih medija za pohranu podataka (CD-ROM, USB uređaji, diskete i sl.) te ostavljanja nezaštićenog pristupa računalu kojim se ostvaruje pristup informacijskom sustavu. U slučaju privremenog napuštanja radnog mjesta korisnik je dužan pokrenuti program koji onemogućuje pristup sustavu bez prethodne autentikacije (*screensaver*). U slučajevima gdje to nije moguće, potrebno je terminirati rad u svim aktivnim aplikacijama ili isključiti računalo. Svi povjerljivi dokumenti i digitalni mediji moraju se spremiti u ormare ili ladice koji su zaštićeni ključem, a posebno nakon radnog vremena. Ostala uredska oprema (telefoni, fax uređaji, fotokopirni aparati, pisači.) koja se nalazi u radnom okruženju također mora biti pravilno zaštićena od neautoriziranog korištenja.

12.8. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

12.9. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

13. Pravila o održavanju

13.1. Ciljevi i opće odredbe

Cilj Pravila o održavanju je određivanje minimalnih zahtjeva za osiguranje kontinuiranosti poslovnog procesa MEF-a.

13.2. Opseg

Ova pravila odnose se na opremu MEF-a i podatke na računalno – komunikacijskom sustavu MEF-a.

13.3. Odgovornost za provedbu

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

13.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju osobe odgovorne za sigurnost na MEF-u i administratori računalnih sustava.

13.5. Održavanje

Integritet i raspoloživost informacija i komunikacijskih servisa nužni su za čitav informacijski sustav. Minimalni zahtjevi koje je nužno ispuniti u cilju osiguranja tih zahtjeva su sljedeći:

- redovito održavanje i bilježenje informacija o radu i pogreškama sustava,
- pohrana i zaštita *(backup)* osjetljivih informacija.

Svu mrežnu, računalnu i programsku opremu potrebno je redovito održavati, na način propisan od proizvođača opreme. Sve nepravilnosti u radu potrebno je dokumentirati.

Sve operativne aktivnosti unutar informatičkog sustava moraju se bilježiti te arhivirati na određeno vrijeme. Svaki zapis o operativnim aktivnostima mora sadržavati sljedeće informacije:

- vremena bitna u radu sustava (pokretanje, zaustavljanje, pogreške, bitne nadogradnje i intervencije…),
- opis obavljenih akcija ili uočenih situacija,
- detektirane pogreške i korektivne akcije,
- ime osobe koja je unijela zapis i vrijeme unosa.

Vrlo je važno bilježenje pogrešaka u radu sustava, te poduzimanje odgovarajućih korektivnih akcija. Procedure kojima se prijavljuju pogreške uočene od strane korisnika također moraju biti definirane (Pravila za rješavanje incidenata i dr.).

13.6. Pohrana i zaštita informacija

Potrebno je uspostaviti detaljne procedure za uspostavu pričuvnih kopija (engl. *Backup)* ključnih poslovnih informacija i programske podrške. Kod implementacije *backup* procedura potrebno je osigurati sljedeće:

- podaci moraju biti pohranjeni zajedno sa svim relevantnim identifikacijskim zapisima i procedurama koje osiguravaju mogućnost obnove svih podataka u odgovarajućem vremenskom roku,
- pohranjeni podaci moraju biti zaštićeni odgovarajućim fizičkim i tehničkim mjerama definiranim od strane MEF-a,
- *backup* medije potrebno je redovito testirati i verificirati,
- efikasnost procedura koje osiguravaju mogućnost obnove mora biti testirana,
- potrebno je definirati vremenske periode koliko je podatke potrebno čuvati; kod toga treba uzeti u obzir i relevantnu pravnu regulativu.

MEF će, također, napraviti procedure i upute za *backup* korisničkih podataka s osobnih računala. Korisnici će biti odgovorni za odabir podataka koji će se *backupirati*, kao i za pokretanje procedure na osobnom računalu.

Za opremu koja sadrži osjetljive informacije (poslužitelji, središnji mrežni uređaji, vatrozid…) potrebno je osigurati nezavisni izvor napajanja, koji će osigurati nesmetan rad opreme neko vrijeme (min. 15 minuta) i sigurnu pohranu podataka u slučaju trajnijeg prekida u opskrbi električnom energijom.

13.7. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

13.8. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

14. Pravila o sigurnosti medija i rukovanju medijima

14.1. Ciljevi i opće odredbe

Sve medije - magnetske, optičke te sistemsku dokumentaciju potrebno je na adekvatan način zaštititi. Mjere zaštite podrazumijevaju kontrolu medija, njihovo označavanje i fizičku zaštitu.

Potrebno je uspostaviti procedure kojima se svi navedeni mediji štite od oštećivanja, neovlaštenog pristupa i krađe.

14.2. Opseg

Ova pravila odnose se na medije za pohranu podataka na računalno – komunikacijskom sustavu MEF-a.

14.3. Odgovornost za provedbu politike sigurnosti informatičkog sustava

Ovaj dokument usvojen je od strane dekana MEF-a. Za njegove provedbu odgovoran je Voditelj sigurnosti, imenovan od strane dekana.

14.4. Obveza pridržavanja

Obavezu pridržavanja ovih pravila ima IT osoblje i svi korisnici računalno – komunikacijskog sustava MEF-a.

14.5. Sigurnost i rukovanje medijima

Postojanje procedura za rukovanje medijima kao što su *floppy* diskete, USB memorije, magnetske trake, CD-RW, CD-ROM, DVD, papirnata izvješća, sistemska dokumentacija itd. je preporučljivo. U skladu s time, potrebno je definirati dozvole za korištenje i prava pristupa medijima. Sve medije potrebno je pohranjivati na za to predviđena mjesta i u skladu sa specifikacijama za njihovo održavanje. Konačno, medije koji više nisu za uporabu potrebno je na ispravan način obrisati ili uništiti.

Da bi se minimizirao rizik od nekontroliranog curenja informacija, potrebno je uspostaviti formalne procedure za uništavanja ili brisanje medija koji se više neće upotrebljavati. Mediji za koje je potrebno definirati te procedure su sljedeći: papirnati dokumenti, sistemska dokumentacija, faksimil poruke, ispisi iz programa, izvješća, prijenosni magnetski mediji, optički mediji i magnetske trake.

Sve papirnate dokumente i izvješća koja sadrže osjetljive informacije potrebno je prije odlaganja fizički uništiti (engl. *shredding*), isto kao i optičke medije. Magnetski mediji

moraju biti obrisani na adekvatan način (višestruko prepisivanje ili *degaussing*). Svako odlaganje medija, odnosno njegovo brisanje ili uništavanje potrebno je dokumentirati.

Za vrijeme životnog vijeka svih ranije navedenih medija, također je preporučljivo definirati odgovarajuće procedure za njihovo rukovanje. Procedure trebaju obuhvaćati slijedeće:

- upute za označavanje i rukovanje,
- kontrolu pristupa i autentikaciju ovlaštenog osoblja,
- formalne zapise o rukovanju medijima,
- pohranu medija u skladu s proizvođačkim specifikacijama,
- označavanje svih kopija,
- regularnu reviziju distribucijskih listi i kanala.

Sistemska dokumentacija, iako to ne mora biti očito,može sadržavati osjetljive podatke kao što su opisi procesa, podatkovnih struktura, procedura i procesa autorizacije. Iz tog razloga i tu dokumentaciju potrebno je štititi kako je opisano.

14.6. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

14.7. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeću

15. Pravila o zaporkama i kriptografskim ključevima

15.1. Ciljevi i opće odredbe

Cilj Pravila o zaporkama i kriptografskim ključevima je određivanje načina rukovanja i obveze čuvanja, odnosno tajnosti zaporki i kriptografskih ključeva.

15.2. Opseg

Ova Pravila odnose se na sve korisnike računalno – komunikacijskog sustava MEF-a, odnosno na sve računalno – komunikacijske resurse koji koriste zaporke ili kriptografske ključeve.

15.3. Odgovornost za provedbu politike sigurnosti informatičkog sustava

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti, kojega imenuje dekan.

15.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju sve fizičke i pravne osobe koje koriste računalno – komunikacijski sustav MEF-a.

15.5. Zaporke

MEF određuje kojim resursima se pristup štiti zaporkama. Procedure za dodjelu zaporki, kao i zahtjeve na izgled zaporke, određuje MEF posebnim dokumentima, a ovdje su dani minimalni zahtjevi na zaporke:

- minimalna duljina zaporke: 6 znakova,
- ne koristiti riječi iz rječnika (riječi sa značenjem),
- ne koristiti imena bliskih osoba, datume…
- izmiješati mala i velika slova te brojeve,
- zaporke treba mijenjati periodički.

Korisnik je odgovoran za tajnost svoje zaporke, ne smije je dijeliti ni sa kim te mora spriječiti njezino doznavanje drugim osobama.

Na sigurnosno osjetljivim resursima, administratori trebaju osigurati da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.

15.6. Kriptografski ključevi

Kriptografski ključevi koriste se prilikom enkripcije podataka. Oni mogu biti generirani automatski ili unaprijed dodijeljeni korisniku. Način generiranja i duljina ključa ovise o osjetljivosti i povjerljivosti štićenih informacija te o primijenjenom kriptografskom algoritmu. Bilo kakvo kompromitiranje ili gubitak kriptografskog ključa vodi do ugrožavanja tajnosti, autentičnosti i/ili integriteta informacija. Upravljanje zaštitom kriptografskih ključeva uključuje zaštitu javnih i tajnih ključeva protiv modifikacije, uništenja te neautoriziranog otkrivanja, a također se mora osigurati i odgovarajuća razina fizičke zaštite opreme koja se koristi za generiranje, spremanje i arhiviranje ključeva.

Procedure i odgovornosti za generiranje, dodjelu, pohranu, poništavanje, obnavljanje izgubljenih ili oštećenih ključeva te za uništavanje ključeva moraju biti definirane.

U primjeni je potrebno definirati vremenski period valjanosti svakog ključa definiranjem datuma aktivacije i deaktivacije ključa.

Korisnici su obvezni voditi računa o svim navedenim aspektima zaštite ključeva te ih, ni u kom slučaju, ne smiju dijeliti s drugim osobama.

15.7. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

15.8. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

SVEUČILIŠTE U ZAGREBU
MEDICINSKI FAKULTET
ZAGREB, Šalata 3

Na temelju članka 152. Statuta Medicinskog fakulteta Sveučilišta u Zagrebu (pročišćeni tekst) u daljnjem tekstu (MEF), dekan donosi sljedeća

16. Pravila za rješavanje incidenata

16.1. Ciljevi i opće odredbe

Cilj ovih Pravila je definiranje ponašanja u slučaju sigurnosnih incidenata na računalno – komunikacijskom sustavu MEF-a.

16.2. Opseg

Ova Pravila odnose se na računalno – komunikacijski sustav MEF-a.

16.3. Odgovornost za provedbu politike sigurnosti informatičkog sustava

Za kontrolu provedbe ovih Pravila zadužen je Voditelj sigurnosti MEF-a, kojega imenuje dekan.

16.4. Obveza pridržavanja

Obavezu pridržavanja ovih Pravila imaju sve osobe odgovorne za sigurnost te korisnici računalno – komunikacijskog sustava MEF-a.

16.5. Prijava incidenta

Svaki korisnik računalno – komunikacijskog sustava MEF-a dužan je prijavljivati incidente i probleme, poput nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa, crva, usporenog rada servisa itd.

Inicdenti se prijavljuju Odsjeku za informatiku, sistemskom administratoru ili osobi odgovornoj za dodjelu prava korištenja opreme na kojoj se incident dogodio. Oni su dužni, u slučaju i najmanje sumnje na sigurnosni incident ili problem, obavijestiti Voditelja sigurnosti, njegovog pomoćnika ili djelatnika Odsjeka za informatičku djelatnost.

MEF će izraditi obrasce za prijavu incidenata. Svaki incident će se dokumentirati, a dokumentacija pohraniti i čuvati najmanje 10 godina.

Voditelj sigurnosti MEF-a odgovoran je za prijavljivanje sigurnosnih incidenata CARNet koordinatoru i CARNet-ovom CERT-u, prema naputcima CERT-a.

16.6. Rješavanje incidenata

U slučaju incidenta Voditelj sigurnosti ima pravo trenutno isključiti računalo iz mreže.

Voditelj sigurnosti ili njegov pomoćnik ili od Voditelja za tu prigodu ovlaštena osoba odgovorna je za rješavanje incidentnih situacija. Odgovorne osobe mogu poduzeti sve korake koje smatraju potrebnim kako bi zaustavili incident ili spriječili njegovo širenje. Pri tome moraju poštovati privatnost korisnika, na primjer ne smiju provjeravati sadržaj korisnikovih datoteka ili elektroničke pošte bez njegove nazočnosti.

Voditelj sigurnosti može naložiti provođenje dodatne istrage (forenzička analiza), uz obavezno dokumentiranje iste i podnošenje izvješća Savjetu za sigurnost. Pri provođenju dodatne istrage moraju se poštivati slijedeća pravila:

- Istragu provodi jedna osoba, ali uz prisustvo svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama.
- Analizirani sustav mora se sačuvati u zatečenom stanju, da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje.
- Najprije treba napraviti kopiju zatečenog stanja (npr. na traku, CD...), po mogućnosti na takav način da se ne izmijene atributi datoteka.
- Dokumentirati svaku radnju, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.
- O istrazi napisati izvještaj, kako bi u slučaju potrebe mogao poslužiti kao dokaz u eventualnim stegovnim ili sudskim procesima.
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na način da im pristup imaju samo ovlaštene osobe.

MEF zadržava pravo objavljivanja statističkih i drugih podataka o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

16.7. Prateći dokumenti

Prateći dokumenti će se donositi po potrebi, a usvojeni dokumenti podložni su revizijama.

16.8. Stupanje na snagu

Ova Pravila stupaju na snagu i primjenjuju se danom objave na oglasnoj ploči Fakulteta.

17. Pravilnik o upravljanju povjerljivim informacijama

17.1. Klasifikacija informacija

Klasificiranje povjerljivih informacija uređeno je Zakonom o zaštiti tajnosti podataka objavljenim u Narodnim novinama br. 114/01. Uskoro se očekuje i zakon o zaštiti osobnih podataka.

Prema vrsti tajnosti informacije dijele se na vojnu, državnu, službenu, poslovnu i profesionalnu tajnu.

Prema stupnju tajnosti, informacije mogu biti povjerljive, tajne ili vrlo tajne.

Kategorije službene, državne i vojne tajne pripadaju tijelima državne uprave.

Poslovna tajna su informacije koje imaju komercijalnu vrijednost i čije bi otkrivanje moglo nanijeti štetne posljedice Ustanovi ili njenim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.)

Profesionalna tajna odnosi na zanimanja poput liječnika, svećenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podacima o drugim ljudima, poput zaposlenih u referadi, osoba koje unose podatke u baze podataka o studentima ili sistem administratora poslužitelja koji u nekim situacijama može doći u dodir s podacima koji pripadaju korisnicima računala.

Dokumenti koji izvana dolaze u Ustanovu s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će Ustanova proizvesti kao odgovor. U tom slučaju može se koristiti neka od kategorija tajnosti koje su rezervirane za tijela državne uprave (službena, državna ili vojna tajna).

Dokumenti koji se smatraju povjerljivima moraju biti jasno označeni isticanjem vrste i stupnja tajnosti.

Javnima se smatraju sve informacije koje nisu označene kao povjerljive. Izuzetak su osobne informacije, za koje se podrazumijeva da su povjerljive i ne treba ih posebno označavati.

Pravila za čuvanje povjerljivosti odnose se na informacije bez obzira na to u kom su obliku: na papiru, u elektroničkom obliku, zabilježene ili usmeno prenesene, ili su objekti poput maketa, slika itd.

17.2. Raspodjela odgovornosti

Za klasificiranje povjerljivih informacija zadužen je u rukovoditelj Ustanove, koji će izraditi listu osoba koje imaju pravo proglasiti podatke tajnima, te listu osoba koje imaju pristup povjerljivim podacima.

Pravila za čuvanje povjerljivih informacija odnose se na sve zaposlenike Ustanove i vanjske suradnike koji dolaze u doticaj sa osjetljivim podacima. Obaveza čuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

Pravilnik o rukovanju povjerljivim informacijama (prijedlog), prosinac, 2003. 27/29 CARNet

Čuvanje povjerljivih informacija

Povjerljive informacije, tiskane na papiru ili u elektroničkom obliku, snimljene na neki medij za pohranu podataka, čuvaju se u zaključanim metalnim, vatrootpornim ormarima, u prostorijama u koje je ograničen pristup.

Pristup povjerljivim informacijama regulira se izradom liste zaposlenika koji imaju ovlasti, te bilježenjem vremena izdavanja i vraćanja dokumenata, kako bi se u svakom trenutku znalo gdje se oni nalaze.

17.3. Informacije o zaposlenicima

Socijalni inženjering je metoda koju primjenjuju hackeri kako bi prikupili informacije potrebne za provalu na računala.

Ustanova može informacije o zaposlenima koje se smatraju javnima objaviti na svojim web stranicama. Javnim informacijama smatraju se:

- ime i prezime
- posao koji zaposlenik obavlja
- broj telefona na poslu
- službena e-mail adresa

Na upite o zaposlenicima davati će se samo informacije objavljene na internim web stranicama. Daljnje informacije o zaposlenima ne smiju se davati bez suglasnosti odobe kojoj podaci pripadaju (na pr. adresa stana, broj privatnog telefona, podaci o primanjima, porezu, osiguranju itd.)

Povjerljive informacije u načelu se ne daju se telefonom jer se sugovornik može lažno predstaviti. Ukoliko se sugovornik predstavlja kao službena osoba koja ima pravo pristupa povjerljivim podacima, zapisuje se ime i prezime te osobe, naziv institucije kojoj pripada i broj telefona s kojeg zove. Nakon provjere istinitosti tih podataka zaposlenik Ustanove će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

17.4. Prenošenje povjerljivih informacija

Informacije koje su klasificirane kao povjerljive zahtijevaju posebne procedure pri slanju i prenošenju.

Povjerljive informacije ne šalju se običnom poštom, već kurirskom. Na odredištu se predaju u ruke osobi kojoj su upućeni, što se potvrđuje potpisom.

Ako se povjerljive informacije šalju elektronički, na primjer kao poruke elektroničke pošte, tada se moraju slati kriptirane.

17.5. Kopiranje povjerljivih informacija

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

Povjerljivi dokumenti koji izvana dođu u Ustanovu ne smiju se kopirati bez izričite dozvole pošiljatelja.

Pravilnik o rukovanju povjerljivim informacijama (prijedlog), prosinac, 2003. 28/29 CARNet Pravilnik o rukovanju povjerljivim informacijama (prijedlog), prosinac, 2003. 29/29

Dokumenti koji pripadaju Ustanovi smiju se kopirati samo uz dozvolu osobe koja ih je proglasila povjerljivim, odnosno uprave. Kopija se numerira i o njenom izdavanju vodi se evidencija kao i za original s kojeg je proizvedena.

Osoblje koje poslužuje uređaje za kopiranje treba obučiti i obavezati da odbiju kopiranje povjerljivih dokumenata ukoliko nije ispoštovana propisana procedura.

17.6. Uništavanje povjerljivih informacija

Mediji koji sadrže povjerljive informacije ne bacaju se, već se uništavaju metodom koja osigurava da se trajno i pouzdano uništi sadržaj (spaljivanjem, usitnjavanjem, prešanjem).

Ukoliko se zastarjela i rashodovana računalna oprema daje na korištenje trećoj strani, obavezno je uništavanje podataka sa diskova posebnim programom koji nepovratno prebriše sadržaj diska.

17.7. Nepridržavanje

Zaposlenici i suradnici koji dolaze u dodir s klasificiranim informacijama potpisuju izjavu o čuvanju povjerljivosti informacija.

Protiv zaposlenika koji ne poštuju pravila o čuvanju povjerljivih informacija bit će pokrenut stegovni postupa, a može ih premjestiti na drugo radno mjesto na kojem neće dolaziti u dodir s povjerljivim podacima.

S vanjskim suradnicima za koje se ustanovi da otkrivaju povjerljive informacije razvrgnuti će se ugovor. Stoga ustanova treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

Broj: 01-70/197-2005

Zagreb, 01. prosinca 2005.

Dekan

Prof. dr. sc. Nada Čikeš