Sigurnosna politika informacijskih sustava Medicinskog fakulteta u Rijeci

UVOD

Koje ciljeve treba postići sigurnosna politika?

Sigurnosna politika dio je sustava upravljanja sigurnošću informacijskih sustava. Njezina je svrha da definira prihvatljive i neprihvatljive načine ponašanja i da jasno raspodijeli uloge i odgovornosti.
Pravila koja su naznačena u ovom dokumentu treba shvatiti kao minimalan skup važećih pravila.

Na koga se odnosi sigurnosna politika?

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- Svu računalnu opremu koja se nalazi u prostorima Medicinskog fakulteta u Rijeci (u daljem tekstu Fakultet)
- Administratore informacijskih sustava (djelatnike službe za informatičku djelatnost)
- Korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti te gosti Fakulteta
- Vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera

Organizacija upravljanja sigurnošću

Ključna stvar pri provođenju sigurnosne politike informacijskog sustava jest da se u svakom trenutku točno zna tko za što odgovara.
Ljudi koji se u radu koriste računalima dijele se na davatelje informacijskih usluga i korisnike.

Davatelji informatičkih usluga

Davateljima se smatraju djelatnici službe za informatičku djelatnost (sistem inženjer i članovi njegova tima). Oni odgovaraju za ispravnost i neprekidnost rada informacijskog sustava. Također, davatelji informatičkih usluga mogu biti i tvrtke od kojih je Fakultet kupio programe i pripadajuće sklopovlje (računala, servere...) te sklopio ugovore o njihovom održavanju.U tim ugovorima moraju biti točno definirane obveze i odgovornosti tvrtke ali i djelatnika službe za informatičku djelatnost. Od odgovornosti službe za informatičku djelatnost za isprvan rad se izuzimaju također računala na koja su priključeni specijalni laboratorijski uređaji i koji su njihov sastavni dio.
Svi detalji oko održavanja moraju biti definirani posebnim ugovorima u koliko Fakultet na bilo koji način surađuje s vanjskim tvrtkama. (kupovina informatičke opreme, programa, servisiranje informatičke opreme i programa, itd.)

Korisnici informatičkih usluga

Svaki korisnik informacijskog sustava mora jasno znati koja je njegova uloga u poboljšanju sigurnosti ukupnog sustava.

Dužnosti korisnika su:

- Pridržavanje pravila prihvatljivog korištenja, to jest da ne koriste računala za radnje koje nisu u skladu sa zakonom i etičkim normama.
- Prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi
- Ukoliko korisnici u svom radu proizvode podatke i dokumente, odgovorni su za vjerodostojnost tih podataka, te za njihovo čuvanje. Moraju sami izrađivati sigurnosne kopije podataka.
  Primjer: u koliko je Fakultet kupio računovodstvene programe od vanjske tvrtke te sklopio ugovor o održavanju recimo servera i programa , ugovor mora sadržavati i stavku o tome da se svaka ugovorna strana mora pridržavati sigurnosne politike odnosno tko je **glavni** korisnik na Fakultetu i koje su njegove obveze. (npr.: tko i kada radi sigurnosne kopije podataka koje su proizišle iz korištenja kupljenog programa)

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, pa treba osigurati njihovo čuvanje i pristup samo ovlaštenim osobama.

Glavni korisnik

Kako Fakultet koristi aplikacije (programe) za obradu podataka, na primjer računovodstvene programe, radi poboljšanja sigurnosti potrebno je imenovati jednu osobu kao glavnog korisnika. U navedenom primjeru voditelj računovodstva bio bi glavni korisnik. Dok njegovi zaposlenici koji unose podatke odgovaraju za vjerodostojnost tih podataka, glavni korisnik odgovaran je za provjeru ispravnosti podataka, za provjeru ispravnosti aplikacije, te za sprečavanje neovlaštenog pristupa podacima, sprečavanje izmjene podataka od strane neautoriziranih osoba. Također, u koliko firma nije programski omogućila automatizirani način pravljenja sigurnosnih kopija podataka, glavni korisnik se zadužuje da ih sam obavlja recimo svaki dan pred kraj radnog vremena.

Pravilnik o korištenju računalne opreme Fakulteta

Svrha pravilnika o korištenju računalne opreme Fakulteta jest da jasno odredi načine na koje je dopušteno koristiti računalnu opremu Medicinskog fakulteta u Rijeci.

- Računalna oprema pripada Medicinskom fakultetu u Rijeci, a korisnicima je dana na raspolaganje radi obavljanja posla.
- Medicinski fakultet u Rijeci zadržava pravo nadzora nad načinom korištenja računalne opreme, kao što je definirano u zasebnom dokumentu, Pravilnik o nadzoru.

Oprema Medicinskog fakulteta u Rijeci koristi se za obavljanje posla. Sve aktivnosti koje nisu povezane sa poslom djelatnika nisu dopuštene.

Nedozvoljenim se smatra svako korištenje računala na način koji bi doveo do povrede zakona, propisa ili etičkih normi, a mogao bi izazvati materijalnu ili nematerijalnu štetu za Medicinski fakultet u Rijeci.

U neprihvatljivo korištenja opreme spadaju:

- Uporaba nelicenciranog softvera
- Skidanje (*download*) autorski zaštićenih datoteka bez plaćanja naknade

- Preuzimanje tuđeg identiteta
  (Korištenje opreme s tuđim korisničkim računom, slanje pošte pod tuđim imenom, kupovanje preko Interneta s tuđom kreditnom karticom itd.)
- Provaljivanje na druga računala
- Traženje ranjivosti i sigurnosnih propusta
  Korisnik ne smije samoinicijativno skenirati računala, probijati zaporke ili na bilo koji način istraživati sigurnosne propuste na računalima, bilo da ona pripadaju Fakultetu ili ne.
- Napad uskraćivanjem resursa na druga računala
- Slanje masovnih poruka, bile one komercijalne prirode ili ne, čime se nepotrebno troše mrežni resursi
- Vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti
- Samovoljna instalacija softvera. Osobe zadužene za instalaciju programa na Fakultetu su djelatnici službe za informatičku djelatnost, čija je obaveza vođenje popisa instaliranog softwarea i briga o licenciranju. Poseban dokument (Pravilnik o instalaciji računala) propisuje točne procedure instalacije i održavanja računala.
- Priključivanje u mrežu Fakulteta svojih privatnih računala i drugih mrežnih uređaja te samovoljno mijenjanje IP adresa odnosno dodijeljivanje istih nekim drugim uređajima. (IP mrežnu adresu dodjeljuje CARNet sistem inženjer i ona pripada isključivo jednom uređaju)
- Postavljanje web stranica na osobna računala
- Instalacija proxy-ja
- Korištenje P2P programa (peer to peer kao sto su: KaZaA, eDonkey, razni torenti itd.)
- Ostavljanje uključenih računala u neradno vrijeme.(računala se nakon završenog radnog vremene isključuju, a ostaju uključena samo ona koja obavljaju specijalne zadaće i moraju biti uključena 24 sata)

Nije moguće nabrojati sve moguće načine neprihvatljivog korištenja računalne opreme, ali za tim nema ni potrebe. Od korisnika se očekuje da sami procijene prihvatljivost svojih postupaka. U slučaju nesigurnosti, neka se obrate za savjet CARNet sistem inženjeru, CARNet koordinatoru, ili drugim osobama iz službe za informatičku djelatnost.

Fizička sigurnost

Sigurne zone

Oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava, ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama.
Npr. kod nas je to prostor u Glavnoj zgradi gdje se nalazi smješten glavni komunikacijski razdjelnik, razdjelnici tel centrale,telefonska centrala te glavni poslužitelj (server:mamed.medri.hr).U taj prostor mogu ući samo djelatnici službe za informatičku djelatnost.
Jedan ključ od gore navedenog prostora je kod Gorana Ružića, a drugi se nalazi na porti Fakulteta.Ključevi (dva ključa) od komunikacijskih ormara također se nalaze na porti Fakulteta. Sve druge osobe kojima se dopusti ulazak u prostor moraju se prilikom preuzimanja ključa(ključeva) sa porte Fakulteta upisati u knjigu intervencija koja se nalazi na porti Fakulteta i to prije i poslije intervencije.

Fakultet je dužan održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone.

Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, a treba predvidjeti i druge moguće probleme, poput poplava, požara i slično, te poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži oporavak.

Vanjske tvrtke

Povremeno se mora dopustiti pristup osobama iz vanjskih tvrtki ili ustanova, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.

Fakultet može u ugovore s vanjskim tvrtkama ugraditi odredbe kojima obavezuje poslovne partnere na poštivanje sigurnosnih pravila.

Ugovorom će se regulirati pristup, čime se podrazumijeva pristup prostorijama, pristup opremi ili logički pristup povjerljivim informacijama. Treću stranu treba obavezati na čuvanje povjerljivih informacija s kojima dođu u dodir pri obavljanju posla.

Fakultet može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, sigurnoj zoni ili osjetljivim informacijama potpiše *Izjavu o čuvanju povjerljivih informacija*.

Ako u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja. Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je osiguran video nadzor.

Ukoliko se vanjskoj tvrtki prepušta održavanje opreme i aplikaicija s povjerljivim podacima, Fakultet može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije Fakulteta radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Fakultet.

Fakultet zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ukoliko nisu na popisu ovlaštenih djelatnika.

Klasifikacija računalne opreme

Fakultet dijeli svu opremu u grupe prema zadaćama koje obavljaju:

Zona javnih servisa (Demilitarizirana zona) – oprema koja obavlja javne servise Fakulteta. (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.).

Intranet je privatna mreža Fakulteta, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže.

Extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili veza između izdvojenih lokacija, zasebnih intraneta. U ovu grupu spadaju na primjer interni modemski ulazi ili veza lokalnih baza podataka s centralnim poslužiteljima (LDAP, ISVU, X-ice).

Podjela opreme prema vlasništvu

U prostorijama Fakulteta nalazi se oprema Fakulteta, ali i oprema CARNeta ili Ministarstva znanosti obrazovanja i športa, koja je dana na korištenje Fakultetu.

Fakultet je obavezan održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarskim brojevima itd.

Fakultet brine jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik. Manirom dobrog gospodara oprema se čuva od oštećivanja, otuđenja.

Pravilnik o antivirusnoj zaštiti

Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka.
Nove generacije virusa su izuzetno složene i opasne, sposobne da prikriju svoje prisustvo, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na Internet, te otvoriti kriptiran kanal do računala, kako bi hackeri preuzeli kontrolu nad njim.
Stoga zaštita od virusa ne smije više biti stvar osobnog izbora, već obaveza Fakulteta, administratora računala i svakog korisnika.
Fakultet propisuje da je zaštita od virusa obavezna i da se provodi na nekoliko razina:

- na poslužiteljima elektroničke pošte
- na internim poslužiteljima, gdje se stavlja centralna instalacija
- na svakom osobnom računalu korisnika

Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju sa centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.
Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti sistem inženjera.

Nepridržavanje
Korisnik koji samovoljno isključi protuvirusnu zaštitu na svom računalu, te na taj način izazove štetu, dužan je naknaditi štetu.

SPAM

Internetom putuje sve više neželjenih komercijalnih poruka, tzv. *spam*. Masovne poruke elektroničke pošte najjeftiniji su način reklamiranja. Cijenu plaćaju korisnici, jer čitanje i brisanje neželjenih poruka troši radno vrijeme i umanjuje produktivnost.

Dio neželjenih poruka nastoji uvući primatelja u kriminalne aktivnosti, na primjer otvaranje računa za pranje novca, ili su prijevara, nastoje pobuditi samilost kako bi se izvukao novac.

Poslužitelj elektroničke pošte konfigurira se tako da prilikom primanja poruka konzultira baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje (open relay), te baza s adresama poznatih spamera. Pošta koja dolazi s tako pronađenih adresa neće se primati.

Druga razina zaštite je automatska provjera sadržaja. Poruke dobijaju bodove koji ukazuju na vjerojatnost da se radi o spamu. Kako nije uvijek moguće pouzdano definirati što je spam, ovakva zaštita mora biti uvjetna, odnosno krajnjem korisniku se prepušta uključivanje bodovanja i konfiguriranje preusmjeravanja označenih poruka.

Pravilnik o nadzoru informacijskih sustava

Fakultet zadržava pravo nadzora nad instaliranim softverom i podacima koji su pohranjeni na umreženim računalima, te nad načinom korištenja računala.

Nadzor se smije provoditi radi:

- osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa.
- provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident.
- provjere da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je Fakultet za to ovlastio (CARNet sistem inženjer i članovi njegovog tima koje on osobno ovlasti).

Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. No u slučaju da je korisnik prekršio pravila sigurnosne politike, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi, te se one mogu koristiti u postupcima pokrenuitim protiv korisnika.

Doseg

Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama Fakulteta i priključena je na lokalnu mrežu i u sveučilišnu mrežu CARNet.

Pravila su dužni poštivati i provoditi svi zaposlenici Fakulteta, studenti i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Provođenje

Korisnici su dužni prijaviti sve probleme u radu informacijskog sustava, poput nedostupnosti podataka, problema u radu mreže i servisa, ali i slučajeve neovlaštenog pristupa, slanje masovnih poruka i sve što se smatra kršenjem pravila prihvatljivog korištenja.

Zaposlenici Fakulteta dužni su pomoći osobama zaduženim za nadzor informacijskih sustava, na taj način što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.

Pristup uključuje:

- Pristup na razini korisnika ili sustava svoj računalnoj opremi
- Pristup svakoj informaciji, u elektroničkom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi Fakulteta, ili oprema Fakulteta služi za njezin prijenos.
- Pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.)
- Pravo na interaktivno nadgledanje i bilježenje prometa na mreži Fakulteta

Nepridržavanje

Zaposlenika koji se ogluši na pravila o nadzoru može se uskratiti pravo korištenja CARNetove mreže i njezinih servisa.

Rješavanje incidenata

Fakultet će izraditi i održavati kontakt listu i obrazac za prijavu incidenta. Na kontakt listi su navedene osobe kojima se prijavljuju problemi u radu informacijskih sustava, njihovo ime i prezime, funkcija, broj telefona, e-mail adresa. Kontakt lista mora biti podijeljena svim zaposlenima.
Fakultet može zatražiti pomoć pri rješavanju incidenata od CARNeta, odnosno tvrtke s kojom CARNet sklopi ugovor o Upravljanjanju sigurnošću mreže.

Svaki incident se dokumentira. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac s opisom incidenta i poduzetih mjera pri rješavanju problema.

Izvještaji o incidentima smatraju se povjerljivim dokumentima, spremaju se na sigurno mjesto i čuvaju 10 godina, kako bi se mogli koristiti kao dokazni materijal u eventualnim postupcima pokrenutim protiv korisnika.

Povjerenstvo za sigurnost razmatra sve incidente i predlaže mjere za sprečavanje sličnih problema u budućnosti.

Incident se prijavljuje CARNetovom CERT-u, preko obrasca na web stranici www.cert.hr.

Procedure za rješavanje incidenata

Osobe koje sudjeluju u istrazi i rješavanju incidenata dužne su čuvati povjerljivost informacija koje tom prilikom otkriju. To se podjednako odnosi na osobne podatke korisnika, kao i na poslovne informacije.

Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedozvoljen način, mogu izlistati sadržaj korisničkog direktorija, ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (na pr. dokumenata ili e-mail poruka).

Daljnju istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost, uz poštivanje slijedećih pravila:

- Istragu provodi jedna osoba, ali uz prisustvo svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama.
- Prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje

- Najprije se napravi kopija zatečenog stanja (na pr. na traku, CD…), po mogućnosti na takav način da se ne izmijene atributi datoteka (na Unixu naredbom dd).
- Dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.
- O istrazi se napiše izvještaj, kako bi u slučaju potrebe mogli poslužili kao dokaz u eventualnim stegovnim ili sudskim procesima.
- Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlaštene osobe.

Ustanova može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

Nepridržavanje

Svi zaposlenici, vanjski suradnici i studenti dužni su pridržavati se pravila i procedura propisanih sigurnosnom politikom.

U slučaju kršenja sigurnosnih pravila protiv zaposlenika se može pokrenuti stegovni postupak za povredu radne obveze, a u najdrastičnijim slučajevima i raskinuti radni odnos. Vanjskim suradnicima može se uskratiti pristup opremi i podacima. Studentima koji krše pravila može se na određeno vrijeme ili trajno uskratiti pravo korištenja CARNetove mreže i usluga. O izricanju takve kazne mora se obavijesti CARNetov CERT.

Ukoliko zaposlenici vanjskih tvrtki koji po ugovoru obavljaju poslove za Fakultet krše sigurnosna pravila, Fakultet im može zabraniti fizički pristup prostorijama ili logički pristup podacima. Fakultet može u ugovore s vanjskim tvrtkama ugraditi stavku po kojoj kršenje sigurnosne politike Fakultet predstavlja dovoljan razlog za raskid ugovora.

Pravilnik o korištenju elektroničke pošte

Elektronička pošta dio je svakodnevne komunikacije, poslovne i privatne. Komuniciranje e-mailom na Fakultetu zahtijeva da se razmotre svi aspekti elektroničke komunikacije s obzirom na moguće posljedice.
Protokol koji se koristi za prijenos elektroničke pošte, SMTP ili Simple Mail Transport Protocol, nije od samog početka dizajniran da bude siguran. Dodatne probleme ponekad izazivaju i korisnici, koji nisu posve svjesni zamki pri korištenju e-maila.
Stoga ćemo se na početku ukratko pozabaviti problemima koji mogu nastati pri korištenju elektroničke pošte.

1. Nesigurnost protokola

   - Poruke putuju kao običan tekst, otvorene kao na razglednici, te ih je lako presresti i pročitati, ili čak izmijeniti sadržaj.
   - Lako je krivotvoriti adresu pošiljatelja, tako da nikada niste sigurni tko vam je zapravo poslao poruku.
   - Protokoli za čitanje elektroničke pošte, POP i IMAP, u svom osnovnom obliku šalju korisničko ime i zaporku kao običan tekst, pa ih je moguće presresti i pročitati. Stoga je potrebno, kad god je to moguće, koristiti kriptografiju, na primjer SSL za prijenos i PGP za skrivanje sadržaja.

2. Nezgode

- uvijek je moguće pritisnuti pogrešnu tipku ili kliknuti mišem na susjednu ikonu. Time može nastati nepopravljiva šteta , a ne možete zaustaviti poruku koja je već otišla. Ako se umjesto Reply pritisne Reply All, poruka će umjesto jednom primatelju otići na više adresa, a povjerljive informacije dospjeti do neželjenih primatelja.
- česta je pogreška i kada se pokupi pogrešna adresa iz adresara.
- neki mail klijenti sami dovršavaju e-mail adresu koju tipkate. U žurbi se može prihvatiti pogrešna adresa, slična onoj koju zapravo želite.

3. Nesporazumi

- korisnici su skloni pisati e-mail poruke na ležerniji, opušteniji način. To može dovesti do nesporazuma ako druga strana ne shvaća poruku na isti način. Stoga službene dopise pišite u službenom tonu.
- iza vašeg imena u e-mail adresi nalazi se ime Fakulteta. Pišući, budite svjesni da netko može shvatiti vašu privatnu prepisku kao službeni dopis, vaše privatno mišljenje kao službeni stav Fakulteta. Stoga u raspravi uvijek jasno naznačite kada je izneseni stav vaše privatno uvjerenje.

4. Otkrivanje informacija

- poruke namijenjene jednoj osobi, začas se mogu proslijediti drugima, na primjer na mailing listu. To se može dogoditi (zlo)namjerno, s ciljem da se naškodi drugoj osobi ili tvrtki nemarom sudionika, koji ne traži dozvolu za prosljeđivanje poruke slučajnom omaškom, na primjer nehotičnim klikom mišem na pogrešnu ikonu (Reply All umjesto Reply)
- Stoga poslovne dopise koji sadrže osjetljive informacije treba označiti kao povjerljive, kako bismo primatelja obavezali na diskreciju.
- U slučaju sigurnosnog incidenta, istraga može dovesti do otkrivanja sadržaja poruka koje su zamišljene kao privatna komunikacija. Fakultet se obavezuje čuvati povjerljivost takvih poruka, ali to ne može garantirati ako poruke budu tretirane kao dokazni materijal u istrazi ili u mogućem sudskom procesu.

5. Radna etika

- Velika količina poruka koje treba svakodnevno pročitati može vam oduzeti znatan dio radnog vremena. Stoga ograničite broj privatnih i zabavnih poruka.
- Lančane poruke koje ljudi šalju poznanicima mogu sadržavati lažne informacije ili biti dio prijevare, s namjerom da se ljudima izvuče novac ("pomozite nesretniku kojem treba operacija“). Za provjeru ovakvih poruka (engl. hoax) može se koristiti servis CARNet CERT-a "Hoax recognizer" (http://www.cert.hr/hoax.php)
- Spam, slanje neželjenih komercijalnih poruka, sve više opterećuje promet na Internetu, te oduzima vrijeme, čak i ako brišete takve poruka bez čitanja. Fakultet će filtrirati spam na poslužitelju elektroničke pošte, ali je obaveza korisnika da sami ne šalju takve poruke.

6. Povreda autorskih prava
- Svaka poruka elektroničke pošte može se smatrati autorskim djelom, stoga ona pripada osobi koja ju je poslala. Stoga za prosljeđivanje tuđe poruke morate tražiti dozvolu njezina autora.
- Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke itd. Primajući i šaljući takve sadržaje možete izložiti tužbi ne samo sebe, već i Fakultet.

Zbog svega nabrojanog korištenje elektroničke pošte smatra se rizičnom djelatnošću, te se korisnici obavezuju na pridržavanje određenih pravila:

- Djelatnicima se otvara korisnički račun radi obavljanja posla.
- Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad. Za privatne potrebe mogu se koristiti za to namijenjeni besplatni davatelji usluga: G-mail, Hotmail, Yahoo mail itd.
- Pišući poruke, budite svjesni da ne predstavljate samo sebe, već i Fakultet.
- Pridržavajte se netikete (ftp://ftp.rfc-editor.org/in-notes/rfc1855.txt), pravila pristojnog ponašanja na Internetu, službenu e-mail adresu nemojte koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno uznemiravanje.
- Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.
- Svaka napisana poruka smatra se dokumentom, te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu. Nemate pravo poruke koju su poslane vama osobno proslijediti dalje bez dozvole autora, odnosno pošiljatelja.
- Sve poruke pregledati će automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni.Nakon određenog vremena poruka se briše iz karantene kako bi se oslobodio prostor na disku.
- Fakultet zadržava pravo filtriranja poruka s namjerom da se zaustave virusi i spam.
- Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.

Korisnici kojima se na poslužitelju Fakulteta može otvoriti korisnički račun podijeljeni su u grupe korisnika i to:

- djelatnici
- vanjski suradnici
- studenti
- gosti

Pri zapošljavanju novog djelatnika, neposredni rukovoditelj zatraži od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa.
Pri prestanku radnog odnosa, neposredni rukovoditelj je dužan najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa. U koliko to ne učini nakon što od Kadrovske službe dobije popis djelatnika koji su raskinuli radni odnos s Fakultetom administrator zatvara korisničke račune.
Studenti imaju pravo besplatnog korištenja e-maila za vrijeme trajanja studija. Nakon što diplomiraju njihov se korisnički račun zatvara i to na način da su ga dužni sami odjaviti. U koliko ga ne odjave, kada od Studentske službe dobije popis studenata koji su diplomirali administrator trajno zatvara njihove korisničke račune.

Fakultet (studentska služba,kadrovska služba) je dužan dostaviti administratoru jedan put mjesečno popise djelatnika odnosno studenata koji su prekinuli radni odnos odnosno završili ili prekinuli studiranje.

Za suradnike i goste voditelj službe ili katedre zatraži od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa i to pismenim putem tj. dokumentom u kojem potvrđuje da je navedena osoba u svojstvu suradnika ili gosta te naznači točno duljinu trajanja korisničkog računa.

Na koga se odnose pravila korištenja e-maila

Pravila za korištenje e-maila odnose se na sve djelatnike, vanjske suradnike, studente te goste koji imaju otvoren korisnički račun na poslužitelju Fakulteta.

Nepridržavanje

U slučaju ponovljenih težih prekršaja, korisniku se može zatvoriti korisnički račun i uskratiti pravo korištenja servisa elektroničke pošte.

Pravilnik o instalaciji i administraciji računala u vlasništvu Medicinskog fakulteta u Rijeci

Osnovne predpostavke za implementaciju ovoga pravilnika su slijedeće:

Sva računala koja Fakultet nabavlja moraju imati predinstaliran licencirani operacijski sustav. Prilikom nabavke računala konzultira se služba za informatičku djelatnost Fakulteta. Ona određuje i preporuča konfiguracije sklopovlja (računala, printera i ostale informatičke opreme)

Instalacija računala:

Instalaciju računala (nadogradnja operacijskog sustava, instalacija licenciranih programa) provodi Informatička služba Fakulteta.

Tijek instalacije:

računalo se ne uključuje u mrežu sve dok se ne učine slijedeći koraci instalacije:

- instalacija - nadogradnja operacijskog sustava (OS) :
- instalacija uslužnih programa
- instalacija sigurnosnih programa

INSTALACIJA

Instalacija operacijskog sustava (OS):

trenutna verzija klijentskog operacijskog sustava je MS XP.

Operacijski sustav instalira se na slijedeći način:

- potrebno je pripremiti instalacijski medij s uključenim zadnjim nadogradnjama operacijskog sustava() ili se zadnje nadogradnje pohrane na poseban medij te nakon osnovne instalacije OS-a iste instaliraju na računalo. Nije dozvoljeno uključiti računalo u mrežu s namjerom instalacije nadogradnji operacijskog sustava.
- nakon provedene instalacije OS-a i pravilne lokalizacije () slijedi postavljanje jedinstvenog passworda (zaporke) za korisnika Administrator. Ovaj pasword za Adminiustratora je jedinstven za sva klijentska računala Fakulteta.
- Sva podešavanja unutar OS-a te instalacija dodatnih uslužnih,sigurnosnih programa te svih ostalih programa izvodi se pod ovlastima korisnika Administrator.

U Control Panel – Folder Options – tab View – Advanced Settings – deselektirati Hide extensions for known file types i Use simple file sharing.
Omogućiti pristup računalu pomoću Remote Dsktop-a i to samo korisniku Administrator.
Izvršiti podešavanje mreže. Mrežne adrese računala dobiju se od Sistem inženjera.

Instalacija uslužnih programa:

uslužne programe čine:

- FilZip – program za komprimiranje sadržaja
- Adobe Reader – program koji omogućuje pregled i čitanje dokumenata u PDF formatu

- MS Java – interpreter Java programa
- CutePdf – program za kreiranje pdf dokumenata
- FireFox – web preglednik

Instalacija sigurnosnih programa:

sigurnosne programe čine (ujedno je to i slijed instalacije):

- Zone Alarm – personal firewall (osobni vatrozid)
- Sophos Antivirus program - antivirusni program

ZoneAlarm program:
nakon osnovne instalacije besplatne verzije programa treba učiniti slijedeća podešavanja:
pod Overview-Preferences-Check for update postaviti na Manually
pod Firewall – Main klizač postaviti na Medium, zatim pod tabom Zones postaviti u TrustedZone slijedeće IP adrese:

161.53.41.1 - 161.53.41.5
161.53.41.44
161.53.41.160
161.53.41.230

pod Alerts & Logs – Main – Alert Events Shown postaviti na Off.

Sophos Antivirus program

instalacija mora biti izvedena na način da omoguči automatsku nadogradnju novih definicija virusa. Kroz Administrative Tools treba prvo kreirati korisnika Sophos i u Local Security Setings-Local policies -User Rights Assignment pod Log on as a service dodati korisnika Sophos.
Time su učinjene predpostavke za početak instalacije Sophos-a.

Računalo se priključuje u mrežu te se pokreće instalacija Sophos-a sa CID-a (dijeljena mapa koja služi samo za instalaciju i ažuriranje antivirusne zaštite umreženih osobnih računala).
Podešavanja programa Sophos:
Pod tabom **Immediate** – meni Options- Configuration-tab Scanning- Scanning level Normal- Priority Normal- uključiti Scan inside archive files i Scan mailboxes,
u tabu Disinfection uključiti: Disinfect boot sectors, Disinfect documents, Disinfect programs, Disinfect mailboxes, Infected files uključiti opciju Delete.
Pod tabom **On- Access** – meni meni Options- Configuration- tab Scanning- Scanning level uključiti Normal i Scan inside archive files, pod tabom Disinfection uključiti: Disinfect boot sectors, Disinfect documents, Disinfect programs i Infected files uključiti opciju Delete. Pod tabom Check uključiti dodatno opciju u dijelu Files – **On Write**.
Ovime je podešavanje programa Sophos Antivirus završeno.
Nakon toga slijedi instalacija licenciranih korisničkih programa i programskih paketa.

Od programskih paketa instalira se jedna od varijanti slijedećih programskih paketa:

- MS Office XP eng
- MS Office XP hrv
- MS Office 2003 eng
- MS Office 2003 hrv
- MS Office 2007 hrv
- MS Office 2007 eng
-

Potrebno je provesti kompletnu instalaciju jednog od gore nabrojanih paketa.

Od programa instalira se program Statistica 7.0.

Nakon ovoga slijedi podešavanje automatizirane nadogradnje operacijskog sustava te jos jednom provjera instaliranih nadogradnji putem mreže.

Na kraju instalacije podešavaju se BIOS postavke i to na način:

- u boot options treba postaviti da se OS može podići samo sa čvrstog diska, a ostale uređaje treba isključiti.

Sve gore navedene instalacije i podešavanja izvode se u prostoru informatičke službe. Računalo se zatim odnosi i priključuje kod korisnika i to u njegovom prisustvu. Korisnik je dužan tom prilikom pripraviti sve dodatne programe koje želi imati instalirane na računalu.Isto se odnosi i na periferne uređaje (printeri, skeneri i sl.). Kad je priključenje računala, perifernih uređaja te instalacija programa konačno gotova, Administrator (djelatnik Informatičke službe) kreira korisnika s minimalnim ovlastima i prepusti korisniku da kreira svoj password za pristup računalu.