Na temelju članka 43. Statuta Filozofskog fakulteta Osijek, Fakultetsko vijeće Filozofskog fakulteta Osijek na 5. sjednici održanoj 26. veljače 2014. donijelo je

PRAVILNIK

o sigurnosnoj politici informacijskih sustava na Filozofskom fakultetu (Sigurnosna politika informacijskih sustava) - pročišćeni tekst -

I. Uvod

Članak 1.

(1) Ovaj Pravilnik donesen je sa svrhom da:
- definira prihvatljive načine ponašanja u svezi s korištenjem informacijskih sustava Filozofskog fakulteta u Osijeku (u daljnjem tekstu: Fakultet)
- raspodijeli zadatke i odgovornosti nadležnih osoba
- utvrdi načine zaštite informacija i podataka koji se u sustavu kreiraju, prenose, obrađuju i pohranjuju
- propiše sankcije u slučaju nepridržavanja odredbi ovog Pravilnika.

(2) Izrazi koji se koriste u ovom Pravilnika, a imaju rodno značenje, koriste se neutralno i odnose se jednako na muški i ženski spol.

II. Opseg primjene

Članak 2.

(1) Ovaj Pravilnik primjenjuje se na sve zaposlene na Fakultetu, vanjske suradnike i studente (u daljnjem tekstu termin *korisnik* odnosi se na sve osobe koje se koriste informacijskim sustavima Fakulteta) kojima se dopušta uporaba računalnih informacijskih sustava Fakulteta.

(2) Pravilnik obuhvaća računalne informacijske sustave Fakulteta i sve sadržaje koji se prenose, pohranjuju i obrađuju u tim sustavima, sadržaje pohranjene na svim osobnim i prijenosnim računalima u vlasništvu Fakulteta, kao i sve poslužitelje koji su u administrativnoj domeni ili vlasništvu Fakulteta.

III. Odgovornost

Članak 3.

(1) Fakultet štiti svoju računalnu opremu, sklopovlje, programsku podršku, podatke i dokumentaciju od zlouporabe, krađe, neovlaštene uporabe i utjecaja okoliša.

(2) Za sigurnost računalnih informacijskih sustava Fakulteta odgovorni su Odjeljak za informatiku i računalnu opremu i korisnici, svako u svom dijelu odgovornosti propisane ovim Pravilnikom.

Članak 4.

Odjeljak za informatiku i računalnu opremu (Ured za informatiku i računalnu mrežu) odgovoran je za sljedeće aktivnosti:

- administriranje i održavanje sigurnosti računalnih informacijskih sustava što uključuje materiju koju uređuje ovaj Pravilnik
- organiziranje i sudjelovanje u svim poslovima vezanim uz informatiku i računalnu mrežu te CARNet
- aktivnosti planiranja, razvijanja i održavanja lokalne mreže
- pružanje odgovarajuće podrške korisnicima prilikom rada na mreži, kao i u ispunjavanju njihove obveze u odnosu na ovaj Pravilnik
- razvijanje i održavanje standarda i procedura kojima se osigurava primjena i pridržavanje odredbi ovog Pravilnika
- za to da sva kritična računalna oprema bude priključena na izvore neprekidnog napajanja, a da ostala oprema bude zaštićena prednaponskom zaštitom
- za sve instalacije, isključivanje, promjene i premještanje računalne opreme (to se ne odnosi na prijenosna računala za koja je početnu konfiguraciju i priključenje u sustav obavio Odjeljak za informatiku i računalnu opremu).

Članak 5.

Korisnici su, glede informacijske sigurnosti, obvezni pridržavati se sljedećih uputa:
- kada nisu u upotrebi, mediji s podatcima i programskom podrškom ne smiju biti izloženi na neovlaštenim osobama lako dostupnim mjestima
- mediji s podatcima i programskom podrškom trebaju se čuvati podalje od nepovoljnih utjecaja okoliša kao što su toplina, izravno sunčevo svjetlo, vlaga, elektromagnetska polja i slično
- utjecaji okoliša kao što su dim, hrana, tekućine, previsoka ili preniska vlažnost te previsoke ili preniske temperature moraju se izbjegavati
- korisnici ne smiju samostalno poduzimati radnje promjene i premještanja računalne opreme
- korisnici prijenosna računala i drugu prijenosnu opremu kojom se koristi više korisnika ne smiju iznositi izvan Fakulteta bez odobrenja dekana Fakulteta
- korisnici se trebaju s pažnjom odnositi prema povjerenoj im računalnoj opremi
- korisnik će se smatrati odgovornim za štete nastale na računalnoj opremi ako su nastale uslijed nepažnje ili nepravilne uporabe.

Članak 6.

Povjerljivost i integritet podataka pohranjenih na računalnim informacijskim sustavima Fakulteta moraju biti zaštićeni sustavom kontrole pristupa kako bi se osiguralo da samo ovlašteni korisnici imaju pristup potrebnim informacijama. Taj pristup treba biti ograničen na samo one informacijske sustave i mogućnosti koje su korisniku nužne za njegove poslovne aktivnosti.

Članak 7.

(1) Svi korisnici obvezni su proučiti i primjenjivati ovaj Pravilnik.
(2) Voditelji ustrojbenih jedinica obvezni su u svojim ustrojbenim cjelinama osigurati da svi korisnici budu upoznati s ovim Pravilnikom te da ga se pridržavaju.

IV. Povjerenstvo za sigurnost informacijskih sustava

Članak 8.

(1) Povjerenstvo za sigurnost informacijskih sustava (u daljem tekstu: Povjerenstvo) imenuje dekan svojom odlukom.
(2) Povjerenstvo se izabire u sljedećem sastavu: jedan zaposlenik Odjeljka za informatiku i računalnu opremu, jedan predstavnik Uprave – prodekan za razvoj i poslovanje, jedan predstavnik

vanjskog davatelja usluge (ako postoji), jedan predstavnik ostalih zaposlenika i jedan predstavnik studenata.
(3) Povjerenstvom predsjedava predstavnik Odjeljka za informatiku i računalnu opremu.

Članak 9.

(1) Povjerenstvo predlaže mjere za poboljšanje sigurnosne situacije, uključujući nabavu potrebne opreme i organizaciju obrazovanja korisnika.
(2) Povjerenstvo pokreće i daje odobrenje za provođenje istrage u slučaju incidenata.
(3) Povjerenstvo Upravi Fakulteta podnosi izvještaj o stanju sigurnosti informacijskih sustava Fakulteta.

V. Administriranje korisnika

Članak 10.

(1) Odjeljak za informatiku i računalnu opremu odgovoran je za administriranje kontrole pristupa računalnom informacijskom sustavu, što uključuje dodavanje, brisanje i promjene prava pristupa korisnicima.
(2) Administriranje korisnika temelji se na zahtjevima:
- Ureda za studentska pitanja
- prodekana za nastavu i studente
- voditelja ustrojbene jedinice u čijoj je organizacijskoj nadležnosti korisnik.

Članak 11.

(1) Pri zapošljavanju novog zaposlenika, neposredni rukovoditelj zatražit će od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa.
(2) Pri prestanku radnog odnosa, neposredni rukovoditelj dužan je najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa. Ukoliko to ne učini, nakon što od Ureda za kadrovske i opće poslove dobije popis zaposlenika koji su raskinuli radni odnos s Fakultetom, administrator zatvara korisničke račune.
(3) Studenti imaju pravo besplatnog korištenja korisničkog računa za vrijeme trajanja studija. Nakon što diplomiraju, njihov se korisnički račun zatvara, i to na način da su ga dužni sami odjaviti. Ukoliko ga ne odjave, kada od Ureda za studentska pitanja dobije popis studenata koji su diplomirali, administrator trajno zatvara njihove korisničke račune.
(4) Ured za studentska pitanja i Ured za kadrovske poslove dužni su dostaviti administratoru jedanput mjesečno popise zaposlenika odnosno studenata koji su prekinuli radni odnos odnosno završili ili prekinuli studiranje.
(5) Za suradnike i goste voditelj službe ili katedre zatražit će 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 uz točno naznačenu duljinu trajanja korisničkog računa.

Članak 12.

(1) Zahtjev se dostavlja putem obrasca *Zahtjev za administriranje korisnika*.
(2) U slučaju hitnosti, brisanja i zabrana prava pristupa mogu se izvršiti i na usmeni zahtjev nadležnog voditelja ustrojbene jedinice, nakon čega mora slijediti i pisani zahtjev kao potvrda.

VI. Administriranje računalne opreme

Članak 13.

(1) Svako računalo mora imati imenovanog administratora koji odgovara za instalaciju i konfiguraciju softvera.
(2) Administrator može naprednim korisnicima odobriti da sami administriraju svoje osobno računalo.

Članak 14.

(1) Računala se moraju konfigurirati na način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpa po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.
(2) Posebnu pažnju potrebno je posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa (npr. serveri, mrežna oprema i slično).
(3) Ugovoreni vanjski davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.

VII. Upravljanje računalnom mrežom

Članak 15.

Upravljanje računalnom mrežom u isključivoj je nadležnosti Odjeljka za informatiku i računalnu opremu i ugovorenih vanjskih davatelja usluge održavanja računalne mreže.

Članak 16.

(1) Odjeljak za informatiku i računalnu opremu mora ažurno voditi dokumentaciju o cjelokupnoj računalnoj mreži Fakulteta, koja se obvezno treba čuvati u metalnom ormaru (kasi) u vrijeme kad se ne koristi.
(2) Ukoliko je dokumentacija o računalnoj mreži u digitalnom formatu, Odjeljak za informatiku i računalnu opremu obvezan je propisati način sigurnog korištenja za davatelje usluge.
(3) Odjeljak za informatiku i računalnu opremu mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala.

Članak 17.

Fakultet treba na prijedlog Odjeljka za informatiku i računalnu opremu propisati pravila za spajanje računala koja sa sobom donose vanjski suradnici, predavači, poslovni partneri i serviseri na računalnu mrežu Fakulteta.

VIII. Zaporke i pristupni računi

Članak 18.

(1) Zabranjuje se korištenje grupnih i univerzalnih pristupnih računa za pristup računalima i računalnim sustavima osim u slučajevima kada je to potrebno za potrebe nastave.
(2) Svaka osoba obvezno mora pristupati računalnom sustavu i računalima Fakulteta isključivo putem vlastitog pristupnog računa osim u slučajevima kada je to potrebno za potrebe nastave.

(3) Izuzetno, Odjeljak za informatiku i računalnu opremu može na pisano traženje dekana ili prodekana za nastavu i studente odobriti korisniku korištenje pristupnim računom druge osobe za pronalaženje i otklanjanje nepravilnosti u radu sustava.
(4) Nakon završetka radnji iz stavka 3 ovoga članka, obvezno treba promijeniti zaporku toga pristupnog računa.

IX. Postupak sa zaporkama

Članak 19.

Korisnik ima sljedeće odgovornosti i obveze:

- odgovoran je za sve računalne transakcije učinjene korištenjem dodijeljenog mu prijavnog imena i zaporke
- ne smije njemu dodijeljene zaporke otkriti drugim osobama
- treba odmah promijeniti svoju zaporku ako posumnja da ju je netko drugi saznao
- ne smije bilježiti zaporke na lako dostupnom mjestu
- treba često mijenjati zaporke
- treba se odjaviti iz informacijskog sustava kada napušta radno mjesto.

Članak 20.

(1) Odjeljak za informatiku i računalnu opremu obvezan je pohraniti sve administratorske zaporke u odgovarajući metalni ormar (kasu) koji treba uvijek držati zaključanim.
(2) Pohranjene zaporke trebaju biti svaka u zasebnoj zapečaćenoj kuverti, na kojoj treba pisati za koji je računalni sustav ili računalnu opremu namijenjena, uz datum kada je posljednji put ažurirana.
(3) Odjeljak za informatiku i računalnu opremu obvezan je redovito nakon svake promjene ažurirati pohranjene zaporke.

X. Računalni virusi

Članak 21.

Odjeljak za informatiku i računalnu opremu ima sljedeće obveze:

- instalirati i održavati odgovarajuće antivirusne programe na svim računalima Fakulteta
- reagirati na svaki napad virusa i uništiti svaki otkriveni virus
- dati upute korisnicima o postupanju glede otkrivenog virusa.

Članak 22.

Obveze korisnika glede računalnih virusa jesu sljedeće:

- ne smiju svjesno unijeti računalni virus u računalni sustav Fakulteta
- trebaju izbjegavati internetske stranice na kojima se pružaju nelegalne usluge, nude piratske kopije računalnih programa, audiosadržaja ili videosadržaja te pornografija
- ne smiju na računalima Fakulteta koristiti podatkovne medije nepoznatog porijekla i sadržaja
- trebaju uz pomoć stručne osobe antivirusnim programom, odobrenim od strane Odjeljka za informatiku i računalnu opremu, pregledati medije koji se unose prije njihove upotrebe
- ukoliko posumnjaju da je računalo zaraženo virusom ili da antivirusna zaštita nije aktivna ili ažurna, moraju računalo odmah isključiti i prijaviti Odjeljku za informatiku i računalnu opremu.

Članak 23.

Uprava Fakulteta obvezna je u pogledu zaštite od računalnih virusa u svom financijskom planu redovito osiguravati dostatna financijska sredstva za nabavu i održavanje programske i sklopovske opreme za zaštitu od njih.

XI. Intelektualno vlasništvo i licenčna prava

Članak 24.

(1) Obveza je Fakulteta i svih korisnika da poštuju zakone i propise o zaštiti intelektualnog vlasništva.
(2) Fakultet je obvezan koristiti se programskom podrškom na temelju valjanih licenčnih prava.
(3) Fakultet programsku podršku i pripadajuću dokumentaciju koja nije u njegovu vlasništvu nema pravo umnožavati i distribuirati bez dopuštenja proizvođača ili autora, osim za potrebe stvaranja sigurnosne kopije.
(4) Na računalima u vlasništvu Fakulteta ne smije se bez odobrenja Odjeljka za informatiku i računalnu opremu koristiti programska podrška nabavljena privatno, bilo kupnjom ili donacijom.

Članak 25.

Odjeljak za informatiku i računalnu opremu ima obvezu:
- održavati ažuran popis programskih licenci u vlasništvu Fakulteta
- čuvati licenčne ugovore ili uvjete korištenja programske potpore
- periodički metodom slučajnog odabira pregledavati računala u vlasništvu Fakulteta radi provjere uporabe samo legalne programske podrške.

Članak 26.

Korisnici ne smiju:
- koristiti programsku podršku na način koji nije u skladu s licenčnim pravima proizvođača
- instalirati aplikacije koje nije odobrio Odjeljak za informatiku i računalnu opremu na računala u vlasništvu Fakulteta
- na računala u vlasništvu Fakulteta instalirati programsku podršku koja nije licencirana ili nije u vlasništvu Fakulteta
- kopirati programsku podršku bez prethodnog odobrenja Odjeljka za informatiku i računalnu opremu
- preuzimati programsku podršku s interneta bez prethodnog odobrenja Odjeljka za informatiku i računalnu opremu.

Članak 27.

(1) Korisnici moraju biti svjesni da kršenje Zakona o intelektualnom vlasništvu može izložiti Fakultet i pojedinca prekršitelja kaznenom postupku koji pokreću nadležna državna tijela neovisno o namjeri Fakulteta.
(2) Korisnici trebaju obavijestiti Odjeljak za informatiku i računalnu opremu o svim zlouporabama programske podrške ili informatičke opreme Fakulteta o kojima imaju saznanja.

XII. Uporaba prostorija podatkovnog centra

Članak 28.

Računalna oprema koja obavlja kritične funkcije neophodne za funkcioniranje informacijskih sustava Fakulteta ili sadrži povjerljive informacije fizički se odvaja u prostor (podatkovni centar) u koji je ulazak dopušten samo ovlaštenim osobama.

Članak 29.

(1) Odjeljak za informatiku i računalnu opremu treba definirati sigurnosna pravila, kao i odrediti pravila ulaska u prostor u kojem je smješten podatkovni centar.
(2) Na taj će se način osigurati siguran pristup i zaštita od neovlaštenog pristupa u prostor podatkovnog centra Fakulteta.

Članak 30.

(1) Ulazak osoba u podatkovni centar treba biti strogo kontroliran.
(2) Odjeljak za informatiku i računalnu opremu utvrđuje popis osoba koje mogu ulaziti u podatkovni centar.

Članak 31.

(1) Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, što znači da električne instalacije moraju biti izvedene kvalitetno te da se koriste uređaji za neprekidno napajanje.
(2) Podatkovni centar treba biti zaštićen od poplava, požara i slično te treba poduzeti mjere da se oprema i informacije zaštite i da se osigura njihov što brži oporavak.
(3) U podatkovnom centru i prostoru oko njega zabranjeno je držanje zapaljivih i eksplozivnih tvari i materijala.

Članak 32.

Ukoliko Fakultet prepušta vanjskoj tvrtki održavanje opreme i aplikacija s povjerljivim podatcima, Odjeljak za informatiku i računalnu opremu odobrava, na temelju potpisanog ugovora, osobama vanjske tvrtke ulazak u prostorije podatkovnog centra Fakulteta radi obavljanja posla.

XIII. Fizička sigurnost opreme

Članak 33.

(1) U prostorijama Fakulteta nalazi se informatička oprema u vlasništvu Fakulteta i oprema CARNeta koja je dana na korištenje Fakultetu.
(2) Odjeljak za informatiku i računalnu opremu odgovoran je za održavanje ažurnog popisa sve računalne opreme s inventarnim brojevima.
(3) Fakultet treba brinuti jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik, čuvajući ju od oštećivanja i otuđenja pažnjom dobrog gospodara.

XIV. Neprekidnost rada

Članak 34.

(1) Kako bi se sačuvali podatci u slučaju nezgoda, poput kvarova na sklopovlju, požara ili ljudskih grešaka, potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera.
(2) Preporučuje se izrada više kopija koje se čuvaju na različitim mjestima, po mogućnosti u vatrootpornim ormarima.
(3) Izrada kopija iz stavka 1. ovog članka *online* preko zasebne računalne mreže ili interneta obvezno se treba izvoditi primjenom odgovarajućeg sustava kriptiranja podataka u prijenosu.

XV. Uporaba lokalne računalne mreže i interneta

Članak 35.

Nije dopušteno, osim, eventualno, u okviru znanstvenog istraživanja:

- stvaranje ili prijenos materijala koji je napravljen da bi izazvao neugodnosti, neprilike ili širio strahove
- distribuiranje autorski zaštićenih djela bez dozvole vlasnika prava, odnosno ostalih informacija bez suglasnosti vlasnika istih
- korištenje tuđeg elektroničkog identiteta ili davanje svojeg elektroničkog identiteta na uporabu drugim osobama
- slanje neželjenih elektroničkih poruka
- slanje elektroničkih poruka većem broju zaposlenika sa sadržajem koji se ne tiče svih zaposlenika kojima se elektronička poruka upućuje
- vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji na temelju vjerske, rasne, nacionalne ili koje druge pripadnosti
- kršenje pravila općeprihvatljivog ponašanja korisnika u komunikaciji pojedinaca ili u grupi na internetu (*netiquette*)
- korištenje mreže na takav način da ometa rad pojedinog servisa ili rad drugih korisnika
- korištenje mrežnih i mrežom dostupnih usluga i servisa protivno pravilima njihove uporabe
- korištenje CARNetovih resursa u komercijalne svrhe
- neovlašteno ostvarivanje prava pristupa ili neovlašteno korištenje pojedinog resursa
- širenje virusa, „trojanaca“ i ostalog zlonamjernog softvera
- kompromitiranje ili neovlašteno uništavanje podataka drugih korisnika
- povreda privatnosti drugih korisnika
- davanje netočnih ili zastarjelih podataka u svrhu ostvarivanja korisničkih prava
- ostavljanje uključenih računala u neradno vrijeme.(računala se nakon završenog radnog vremena isključuju, a ostaju uključena samo ona koja obavljaju specijalne zadaće i moraju biti uključena 24 sata)
- korištenje računalne opreme na ostale neprihvatljive načine
- svako neprihvatljivo korištenje CARNetovih resursa, čije je korištenje propisano CARNetovim CDA-dokumentima.

Članak 36.

(1) Odredba članka 35. odnosi se na sve zaposlene, studente, vanjske suradnike i sve druge osobe kojima se dopušta uporaba računalnih informacijskih sustava Fakulteta korištenjem lokalne mreže i Interneta.
(2) Od svih korisnika očekuje se da budu upoznati s odredbom članka 35. ovog Pravilnika i da ju u svakodnevnom radu poštuju, te su slijedom toga odgovorni za njezinu primjenu.

Članak 37.

Odgovornost i obveze administratora ogledaju se u sljedećim stavkama:

- uspostavljanju i održavanju sigurnosnih pravila i standarda te davanju tehničke potpore korisnicima Fakulteta pri uporabi lokalne mreže i interneta
- organiziranju i provođenju reakcije na moguće krizne situacije u računalnom sustavu Fakulteta (zaraza računalnim virusom, napad hakera i sl.)
- provođenju periodičke procjene sigurnosnih rizika na svim produkcijskim sustavima koji su u njegovoj odgovornosti
- provjeri sigurnosnih mjera implementiranih na tim sustavima i utvrđivanju odgovaraju li one razini osjetljivosti informacija pohranjenih u njima
- osiguravanju pristupnih prava pojedinih korisnika na najmanjoj razini potrebnoj za njihov rad
- nadziranju uporabe interneta, detektiranju mogućih kršenja odredbi ovog Pravilnika te izvještavanju Odjeljka za informatiku i računalnu opremu o tim pojavama.

Članak 38.

Korisnici računalnih sustava Fakulteta moraju:

- poznavati i primjenjivati odredbe ovog Pravilnika
- zapriječiti neovlaštenim pojedincima pristup u lokalnu mrežu Fakulteta te dalje u javnu računalnu mrežu, tj. internet
- održavati tajnost uporabe svojih pristupnih zaporki za mrežne usluge i zaštititi ih od nenamjernog otkrivanja drugim osobama
- Odjeljku za informatiku i računalnu opremu prijaviti svaku pojavu za koju se čini da narušava sigurnost informacijskih sustava Fakulteta pri korištenju lokalne mreže ili interneta (virusne zaraze, neobjašnjive transakcije, nedostajuće podatke, neovlašteno ili zabranjeno skidanje programa, audiosadržaja, videosadržaja i slično)
- pristupati samo podatcima i funkcijama za koje su slijedom redovnih poslovnih aktivnosti ovlašteni
- tražiti ovlaštenje od nadležnih osoba za sve aktivnosti koje izlaze iz okvira korisnikovih redovnih poslovnih aktivnosti, posebno za aktivnosti razmjene podataka s osobama i sustavima izvan Fakulteta.

XVI. Uporaba elektroničke pošte

Članak 39.

Svrha ovih odredbi Pravilnika jest utvrditi smjernice, postupke i zahtjeve za osiguravanje prihvatljivih načina uporabe sustava elektroničke pošte Fakulteta te zaštitu informacija i resursa Fakulteta od zlouporabe korištenjem elektroničke pošte.

Članak 40.

(1) Ove odredbe odnose se na sve zaposlene, vanjske suradnike, studente, gostujuće profesore i studente te sve druge osobe kojima je dopuštena uporaba računalnih informacijskih sustava Fakulteta.
(2) Ove odredbe primjenjuju se na sustav elektroničke pošte i sve poruke elektroničke pošte smještene na osobna računala u vlasništvu Fakulteta, kao i sve poslužitelje elektroničke pošte u administrativnoj domeni ili vlasništvu Fakulteta.
(3) Odredbe se odnose i na sva računala u vlasništvu Fakulteta, priključena u računalnu mrežu Fakulteta ili samostalna računala priključena na internet pomoću drugih veza.

Članak 41.

(1) Odgovornost za primjenu ovih odredbi imaju svi korisnici.
(2) Korisnici elektroničke pošte obvezuju se na poštivanje određenih pravila:
- zaposlenicima se korisnički račun otvara radi obavljanja posla
- privatne poruke dopuštene 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.
- pridržavajte se *netikete* (ftp://ftp.rfc-editor.org/in-notes/rfc1855.txt), pravila pristojnog ponašanja na internetu, te se službenom adresom e-pošte nemojte koristiti za slanje uvredljivih i omalovažavajućih poruka ili za seksualno uznemiravanje
- nije dopušteno slanje lančanih poruka kojima se opterećuju mrežni resursi i djelatnicima 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
- prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, naprimjer glazbu, filmove, članke itd., pa primajući i šaljući takve sadržaje možete izložiti tužbi ne samo sebe već i Fakultet.
- sve poruke automatski će pregledati aplikacija koja otkriva viruse; ako poruka zadrži virus, neće biti isporučena, a pošiljatelj i primatelj bit će o tome obaviješteni; poruka će provesti određeno vrijeme u karanteni, a 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 tijekom propisanog razdoblja kao i dokumente na papiru.

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

Članak 42.

Administrator mora:
- uspostaviti i održavati sigurnosna pravila i standarde te korisnicima davati tehničku podršku pri uporabi sustava elektroničke pošte
- nadzirati rad i uporabu sustava elektroničke pošte, detektirati moguća kršenja ovih odredbi te o tome izvijestiti dekana Fakulteta
- u slučaju sumnje u moguće počinjenje kaznenoga djela ili odavanja poslovnih informacija obaviti nadzor sadržaja sandučića elektroničke pošte zaposlenika te izvršiti kopiranje potrebnog sadržaja.

Članak 43.

Voditelji ustrojbenih jedinica moraju u svojim ustrojbenim cjelinama osigurati da svi korisnici elektroničke pošte budu upoznati s odredbama ovog Pravilnika te da ih se pridržavaju.

XVII. Uporaba prijenosnih računala

Članak 44.

(1) Odredbe ovog Pravilnika primjenjuju se u cijelosti i na korištenje prijenosnih računala u vlasništvu Fakulteta te prijenosnih računala drugih vlasnika koja se priključuju na lokalnu mrežu Fakulteta.

(2) Odredbe se odnose na sve zaposlene na Fakultetu, vanjske suradnike i studente koji se koriste privatnim ili službenim prijenosnim računalom kao sredstvom rada na Fakultetu.

XVIII. Objavljivanje informacija putem računalne mreže

Članak 45.

Odredbama ovoga poglavlja regulira se objavljivanje informacija putem računalne mreže i interneta, a svrha im je davanje smjernica za poslovanje, postupke i zahtjeve za osiguranjem prihvatljivih načina uporabe računalne mreže i interneta za interno i javno objavljivanje informacija na mrežnim stranicama Fakulteta, Fakulteta na društvenim mrežama, uključujući odredbe za administriranje mrežnih stranica intraneta i interneta, mrežnih stranica na društvenim mrežama te zaštitu informacija i resursa Fakulteta od zlouporaba.

Članak 46.

(1) Odredbe se odnose na zaposlene, studente, vanjske suradnike, gostujuće studente i sve druge osobe kojima je dopuštena uporaba računalnih informacijskih sustava Fakulteta za objavljivanje informacija na mrežnim stranicama Fakulteta.
(2) Odredbe obuhvaćaju sustav za administriranje mrežnih stranica intraneta, mrežnih stranica javne mreže, Fakulteta na društvenim mrežama te sve poslužitelje koji su dio tog sustava, a u administrativnoj su domeni ili vlasništvu Fakulteta.

Članak 47.

(1) Dekan svojom odlukom formira Uredništvo javnih mrežnih stranica Fakulteta, koje je odgovorno za objavljivanje informacija na mrežnim stranicama Fakulteta.
(2) Uredništvo čine glavni urednik i članovi koje imenuje dekan Fakulteta.

Članak 48.

Uredništvo mrežnih stranica:
- definira i objavljuje upute za objavu informacija na mrežnim stranicama
- određuje strukturu informacija na mrežnim stranicama te definira stupnjeve ovlasti za rad sa sustavom
- predlaže i nadzire vizualnu i sadržajnu ujednačenost objavljenih informacija
- nadzire korektnost objavljenih informacija te korektnost uporabe sustava od strane korisnika
- vodi popis osoba imenovanih za uređenje mrežnih stranica Fakulteta i odsjeka
- prati posjećenost mrežnih stranica s ciljem unapređenja kvalitete rada Fakulteta.

Članak 49.

Obveze glavnog urednika jesu:
- davanje ovlaštenja korisnicima za pristup pojedinim dijelovima sustava
- koordiniranje aktivnosti vezanih uz ispravnost funkcioniranja tehničke podrške sustava
- briga o statistikama administriranja i posjećenosti mrežnih stranica koje se koriste u svrhu unapređenja sustava
- nadziranje ispravnost funkcioniranja sustava
- predlaganje i provođenje sigurnosnih mjera koje osiguravaju zaštitu od neovlaštenog korištenja podataka i neovlaštenog objavljivanja informacija.

XIX. Upravljanje povjerljivim i važnim podatcima

Članak 50.

(1) Odredbama ovoga poglavlja regulira se način zaštite povjerljivih računalnih podataka kojima se koristi Fakultet od neovlaštenog pristupa i korištenja od strane trećih osoba.
(2) Odredbe se odnose na sve voditelje ustrojbenih jedinica i sve korisnike koji na bilo koji način raspolažu povjerljivim informacijama ili dolaze u kontakt s njima.

Članak 51.

Voditelji ustrojbenih jedinica obvezni su voditi brigu o ograničenoj dostupnosti povjerljivih informacija i podataka korisnicima u njihovoj ustrojbenoj jedinici, a posebno brinuti o sljedećem:

- da korisnici brišu osjetljive (povjerljive) informacije sa svojih diskova i drugih vanjskih memorijskih komponenti kad im ti podatci više nisu potrebni za rad
- da korisnici snimaju i pohranjuju svoje zaštitne kopije važnih informacija u skladu s razinom važnosti informacija
- da korisnici kojima prestaje radni odnos na Fakultetu prođu postupak razduživanja informatičke opreme i pohranjenih povjerljivih i važnih podataka prije napuštanja Fakulteta
- da osiguraju da podatci pod kontrolom korisnika budu pravilno zaštićeni, u skladu s razinom osjetljivosti informacija.

XX. Rješavanje sigurnosnih incidenata

Članak 52.

(1) Odredbe ovoga poglavlja reguliraju obvezu prijavljivanja sigurnosnih incidenata te utvrđuju procedure za provođenje istrage.
(2) Svaka osoba zaposlena na Fakultetu, kao i svaki student i vanjski suradnik, dužni su prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.

Članak 53.

(1) Odjeljak za informatiku i računalnu opremu treba odrediti osobu kojoj se prijavljuju problemi u radu računala i servisa te načiniti obrazac za prijavu incidenta koji sadržava kratak opis incidenta i poduzete mjere pri rješavanju problema.
(2) Odluku o imenovanoj osobi s kontakt-podatcima treba objaviti na oglasnoj ploči, kao i na internim mrežnim stranicama Fakulteta.
(3) Svaki se incident dokumentira.
(4) 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.

Članak 54.

(1) 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.
(2) Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedopušten način, mogu izlistati sadržaj korisničkog direktorija, ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (npr. dokumenata ili poruka e-pošte).

(3) Daljnja istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost informacijskih sustava, 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 (npr. na vrpcu, CD…), po mogućnosti na takav način da se ne izmijene atributi datoteka
- dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage
- o istrazi se napiše 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 mogu pristupiti samo ovlaštene osobe

(4) Fakultet može objavljivati statističke podatke o sigurnosnim incidentima bez otkrivanja povjerljivih i osobnih informacija.

XXI. Antivirusna zaštita i zaštita od neželjene pošte

Članak 55.

(1) Zaštita od virusa obveza je Fakulteta, administratora i svakog korisnika.
(2) Odredbe ovoga poglavlja utvrđuju kako osigurati i provoditi sustavnu zaštitu od zlonamjernih programa (virusa) i neželjene elektroničke pošte (*spama*).

Članak 56.

Zaštita od virusa obvezno se provodi na više razina:

- na poslužiteljima elektroničke pošte
- na svim poslužiteljima poslovnih i javnih servisa
- na svakom osobnom računalu.

Članak 57.

Administrator je dužan instalirati antivirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski apliciraju sa središnje instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.

Članak 58.

Administrator poslužitelja elektroničke pošte dužan je konfigurirati računala na način da se što više neželjenih poruka zaustavi i preusmjeri u mapu neželjenih poruka.

Članak 59.

(1) Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu.
(2) Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju o tome obavijestiti administratora.

XXII. Rukovanje zaporkama

Članak 60.

Svi zaposleni na Fakultetu, vanjski suradnici i studenti koji se u svome radu koriste računalima dužni su pridržavati se pravila korištenja zaporki, dok ih je administrator dužan tehnički ugraditi u sve sustave koji to omogućavaju. Na taj način osigurat će se sigurno korištenje i čuvanje zaporki na svim razinama i za sve informacijske sustave u uporabi na Fakultetu.

Članak 61.

(1) U kreiranju svih potrebnih zaporki – korisničke zaporke, administratorske zaporke, zaporke potrebne za pristup Fakultetu izvana, zaporke trećih osoba koje pristupaju Fakultetu, zaporke za pristupanje elektroničkoj pošti - svi su korisnici (zaposleni, vanjski suradnici, studenti, treće osobe) dužni voditi računa o sljedećim tehničkim specifikacijama:
- zaporka mora sadržavati najmanje osam alfanumeričkih znakova
- zaporka mora sadržavati najmanje jedno veliko slovo, najmanje jedan broj i najmanje jednu interpunkciju
- nove zaporke moraju biti različite od tri zadnje koje su se upotrebljavale i od zaporki koje su upotrebljavane u zadnjih godinu dana
- korisnici moraju imati mogućnost mijenjanja vlastite zaporke samostalno i bez nadgledanja
- zaporke ne smiju biti prikazane na ekranu u čitljivom obliku prilikom unosa
- prilikom kreiranja korisničkog računa, prvu postavljenu korisničku zaporku korisnik je dužan promijeniti kad se prvi put prijavi u sustav
- zaporke se ne smiju kreirati površno (ne upotrebljavati imena članova obitelji, kućnih ljubimaca, kolega s posla, prijatelja, datume rođenja, pojmove vezane uz djelatnost i sl.)
- uvijek se moraju koristiti različite zaporke za korisničke račune od onih zaporki koje se koriste za privatne korisničke račune
- ne smije se prihvatiti mogućnost "Zapamti moju zaporku" (eng. "Remember Password") pri korištenju različitih aplikacija
- ukoliko korisnik unese četiri puta pogrešnu zaporku, korisnički račun će mu biti automatski blokiran
- u slučaju da je korisnik neaktivan na računalu u periodu od petnaest minuta, računalo se mora automatski zaključati zaporkom.

(2) Korisnici su odgovorni za svoju zaporku i ni u kojem ju slučaju ne smiju otkriti, čak ni administratorima sustava

XXIII. Prekršaji i sankcije

Članak 62.

(1) Svi korisnici računalnih informacijskih sustava Fakulteta dužni su pridržavati se odredbi ovog Pravilnika, kao i svih drugih internih odluka koje reguliraju korištenje računalnih informacijskih sustava i informatičke opreme.
(2) Kršenje odredbi ovog Pravilnika može korisnika izložiti zabrani prava uporabe računalnih informacijskih sustava Fakulteta te pokretanju stegovnog postupka sve do prestanka ugovora o radu iz razloga uvjetovanog krivim ponašanjem radnika ili prestanka drugih ugovora.

Članak 63.

(1) O zabrani prava uporabe računalnih informacijskih sustava Fakulteta te pokretanju stegovnog postupka odlučuje dekan na prijedlog Odjeljka za informatiku i računalnu opremu.
(2) Sankcije za učinjenu povredu, odnosno korištenje računalnim informacijskim sustavima Fakulteta protivno odredbama ovog Pravilnika, ovisit će o vrsti i veličini prekršaja, zatim o tome je li prekršajem uzrokovana pravna, materijalna ili kakva druga šteta te radi li se o prvom ili ponovljenom prekršaju.

Članak 64.

Ovaj Pravilnik stupa na snagu osmog dana od dana objave na oglasnoj ploči Fakulteta.

DEKANICA
prof. dr. sc. Loretana Farkaš

Ovaj Pravilnik objavljen je na oglasnoj ploči Fakulteta 27. veljače 2014. godine te je stupio na snagu 6. ožujka 2014. godine.

Na temelju točke 3. Odluke o izmjenama i dopunama Pravilnika o sigurnosnoj politici informacijskih sustava na Filozofskom fakultetu (Sigurnosna politika informacijskih sustava), Tajništvo Fakulteta utvrdilo je dana 12. studenoga 2018. godine pročišćeni tekst Pravilnika o sigurnosnoj politici informacijskih sustava na Filozofskom fakultetu (Sigurnosna politika informacijskih sustava). Pročišćeni tekst Pravilnika o sigurnosnoj politici informacijskih sustava na Filozofskom fakultetu (Sigurnosna politika informacijskih sustava) obuhvaća Pravilnik o sigurnosnoj politici informacijskih sustava na Filozofskom fakultetu (Sigurnosna politika informacijskih sustava) od 26. veljače 2014. godine, Odluku o izmjenama i dopunama Pravilnika o sigurnosnoj politici informacijskih sustava na Filozofskom fakultetu (Sigurnosna politika informacijskih sustava) od 24. rujna 2014. godine, Odluku o izmjenama i dopunama Pravilnika o sigurnosnoj politici informacijskih sustava na Filozofskom fakultetu (Sigurnosna politika informacijskih sustava) od 17. siječnja 2018. godine i Odluku o izmjenama i dopunama Pravilnika o sigurnosnoj politici informacijskih sustava na Filozofskom fakultetu (Sigurnosna politika informacijskih sustava) od 7. studenoga 2018. godine u kojima je naznačeno vrijeme stupanja na snagu.

TAJNICA
Narcisa Vrbešić-Ravlić, mag. iur.

KLASA: 003-05/18-01/1
URBROJ: 2158-83-02-18-3