SVEUČILIŠTE U SPLITU
FILOZOFSKI FAKULTET

PRAVILNIK
O SIGURNOSTI INFORMACIJSKIH SUSTAVA
FILOZOFSKOG FAKULTETA U SPLITU

Split, lipanj 2018. godine

Temeljem članka 46. Statuta Filozofskog fakulteta u Splitu (pročišćeni tekst, ožujak 2018.), sukladno odredbama Uredbe (EU) 2016/679 od 27. 4. 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ te odredbi Zakona o provedbi Opće uredbe (NN, br. 42/18), Fakultetsko vijeće Filozofskog fakulteta u Splitu na 14. virtualnoj sjednici u akad. god. 2017./2018. održanoj 29.5. do 1.6. 2018. godine, donosi

PRAVILNIK
o sigurnosti informacijskih sustava Filozofskog fakulteta u Splitu

Uvodne odredbe

Članak 1.

Ovim se Pravilnikom uređuje sigurnost upravljanja informacijskim sustavima na Filozofskom fakultetu u Splitu (dalje: Fakultet), definiraju prihvatljivi načini ponašanja i jasna raspodjela uloga i odgovornosti svih čimbenika informacijskog sustava.

Novi zaposlenici dužni su se upoznati s njegovim odredbama prilikom zapošljavanja, a studenti prilikom otvaranja korisničkih računa.

Pravila rada i ponašanja odnose se na:

- svu računalnu opremu koja se koristi u prostorima Fakulteta,
- administratore informacijskih sustava,
- korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti, polaznici
- vanjske tvrtke i/ili ustanove koje po ugovoru rade na održavanju opreme ili informacijskih sustava (npr. aplikacije).

Organizacija upravljanja sigurnošću

Članak 2.

Osobe koji se u radu koriste računalima dijele se na davatelje i korisnike informatičkih usluga.

Davateljima informatičkih usluga smatraju se profesionalci koji brinu o radu računalne opreme (u daljnjem tekstu: računala), mreže i informacijskih sustava. Davatelji informatičkih usluga mogu biti zaposlenici Fakulteta (u daljnjem tekstu: davatelji usluga na Fakultetu) ili zaposlenici vanjskih tvrtki i/ili ustanova koje po ugovoru rade na održavanju opreme ili informacijskih sustava (u daljnjem tekstu: vanjski davatelji usluga).

Korisnici informatičkih usluga su osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže. Korisnici informatičkih usluga (u daljnjem tekstu: korisnici) dužni su:

- pridržavati se pravila prihvatljivog korištenja, to jest ne koristiti računala za radnje koje nisu u skladu sa važećim propisima kojima je regulirana predmetna materija i uputama davatelja informatičkih usluga na Fakultetu,
- izabrati zaporku i povremeno je mijenjati,
- prijaviti svaki sigurnosni incident,
- ako korisnici u svom radu proizvode podatke i dokumente, odgovorni su za vjerodostojnost tih podataka te za njihovo čuvanje i izradu sigurnosnih kopija.

Sve osobe koje se koriste računalima za obradu osobnih podataka i dokumenata obvezne su postupati prema utvrđenim procedurama u skladu s odredbama Uredbe EU 2016/679 Europskog parlamenta i vijeća od 27. 4. 2016. (u daljnjem tekstu: Opća uredba o zaštiti podataka).

Članak 3.

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

Članak 4.

Svaka aplikacija koju Fakultet koristi za obradu podataka, a koja je od vitalne važnosti za Fakultet ili njegov dio, mora imati glavnog korisnika.

Glavni korisnik je zaposlenik koji primarno koristi tu aplikaciju u sklopu obavljanja svojih poslovnih zadaća.

Svi zaposlenici koji koriste aplikaciju za obradu podataka odgovorni su za ispravnost i ažurnost podataka koje unose te usklađenost obrade podataka s odredbama Opće uredbe o zaštiti podataka.

Davatelji usluga odgovorni su za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprečavanja izmjene podataka od strane neautoriziranih osoba. Glavni korisnik kontaktira vanjskog davatelja usluge u vezi redovitog održavanja aplikacije i sigurnosti.

Potrebnu nadogradnju, isporuku novih verzija, ugradnju sigurnosnih mehanizama i sl. s vanjskim davateljima usluga dogovaraju i koordiniraju davatelji usluga na Fakultetu.

Članak 5.

Osoba čije je prvenstvena briga sigurnost informacijskih sustava je voditelj davatelja usluge na Fakultetu (u daljnjem tekstu: voditelj sigurnosti).

Briga voditelja sigurnosti je ukupna sigurnost informacijskih sustava, koja uključuje i fizičku sigurnost.

Voditelj sigurnosti nadzire rad mreže i servisa, koordinira obrazovanje korisnika i administratora, komunicira s upravom, sudjeluje u donošenju relevantnih propisa i provedbi postupka nabave računalne opreme i aplikacija, a sve u svrhu osiguranja sigurnosti informacijskih sustava na Fakultetu.

Članak 6.

Voditelj sigurnosti treba izraditi i održavati kontakt listu s imenima, brojevima telefona, email adresama osoba kojima se prijavljuju incidenti, od kvarova mrežne opreme, sporosti ili nedostupnosti mrežnih usluga i podataka, do povreda pravila sigurnosnih standarda ili zakonskih odredbi.

Članak 7.

Davatelji usluga na Fakultetu dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

Svako računalo mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju softvera. Ako napredni korisnici žele sami administrirati svoje osobno računalo, neka potpišu izjavu o tome, nakon čega za njih vrijede sva pravila za administriranje računala. Voditelj sigurnosti evidentira zaduženja administratora po računalima.

Računala se moraju konfigurirati na taj način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.

Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa.

Članak 8.

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

Administratori su dužni prijaviti incidente voditelju sigurnosti te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ukoliko je incident ozbiljan i uključuje kršenje zakona, prijavljuju se CARNetovu CERT-u.

Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla te moraju potpisati Izjavu o čuvanju povjerljivih informacija.

Članak 9.

Upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje mrežnih adresa, kreiranje virtualnih LAN-ova te ostale poslove pri upravljanju mrežom obavlja davatelj usluge na Fakultetu.

Zahtjev za priključivanje računala na mrežu daje se isključivo davatelju usluge na Fakultetu koji provodi daljnje korake za priključivanje računala na mrežu.

Davatelj usluge na Fakultetu je dužan voditi Popis mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala. Administratori CARNet-ovih poslužitelja dužni su voditi Popis javnih adresa računala.

Članak 10.

Gostujuća računala smiju se priključiti na lokalnu mrežu samo na za to predviđenim mjestima (informatičke učionice, predavaonice, hodnik, knjižnica i sl.), a bežično na izdvojenim lokalnim Wifi mrežama.

Uvjeti i načini korištenja bežičnih mrežnih resursa, metode enkripcije i autentifikacije uređaja i korisnika te ostale sigurnosno važne postavke definirani su standardima korištenja Eduroam mreža.

Članak 11.

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Korisnik koji ima potrebu za nekim programom, mora se obratiti davatelju usluge na Fakultetu i zatražiti, uz obrazloženje, nabavu i instalaciju.

Članak 12.

Voditelj sigurnosti daje godišnje izvještaje dekanu o sigurnosnoj situaciji i predlaže mjere za njeno poboljšanje, za nabavu opreme i obrazovanje davatelja usluge na Fakultetu te korisnika. U slučaju incidenata provodi istragu.

U slučaju sigurnosnog incidenta prouzrokovanog od strane osoba koje nisu fakultetski korisnici, voditelj sigurnosti daje CARNet koordinatoru nalog za prijavu sigurnosnog incidenta CERT-u koji se nalazi u sastavu CARNet-a.

Fizička sigurnost

Članak 13.

Prostor na ustanovi dijeli se na dio koji je otvoren za javnost te prostore u koje pristup imaju samo grupe zaposlenih, ovisno o vrsti posla koji obavljaju.

Voditelj sigurnosti kreira, vodi i održava popis osoba koje imaju pristup u zaštićena područja, a osoblje na portirnici mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Članak 14.

Oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava ili sadržava povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama.

Voditelj sigurnosti je dužan održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone. U pravilu su to samo zaposlenici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje, obaviti servisiranje opreme.

Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, poplava, požara i sl. te treba poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži oporavak. U

sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Članak 15.

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

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.

Sigurnost opreme

Članak 16.

Fakultet dijeli svu aktivnu i pasivnu opremu u grupe prema zadaćama:

- ***zona javnih servisa*** - oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.), i
- ***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 povezuje izdvojene lokacije; u ovu grupu spadaju veze lokalnih baza podataka sa središnjim poslužiteljima (LDAP, ISVU, X-ice, baze knjižnice) i sl.

Članak 17.

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

Fakultet je dužan osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi na Fakultetu.

Voditelj sigurnosti prenosi odgovornost za fizičku sigurnost opreme (za grupe uređaja ili pojedine uređaje) na druge zaposlenike, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.

Računalna oprema koja pripada Fakultetu daje se korisnicima na raspolaganje radi obavljanja poslova vezanih uz redovno poslovanje Fakulteta i nije ju dopušteno koristiti za obavljanje privatnih poslova korisnika.

Fakultet zadržava pravo nadzora nad načinom korištenja računalne opreme.

Privatna računala i računalnu opremu je dopušteno priključivati na lokalnu računalnu mrežu Fakulteta samo na za to predviđenim mjestima, sukladno utvrđenom člankom 10. ovog Pravilnika.

Računala i računalnu opremu nije dopušteno iznositi izvan prostora Fakulteta bez uredno ovjerene Potvrde o korištenju opreme izvan Fakulteta. Potvrdu izdaje voditelj sigurnosti, na obrazloženi zahtjev korisnika. Korisnici koji opremu koriste izvan prostora Fakulteta odgovorni su za tu opremu kao i za sve posljedice koje proizlaze iz korištenja iste.

Osiguranje neprekidnosti poslovanja

Članak 18.

Kako bi se sačuvali podaci u slučaju nezgoda, kvarova na sklopovlju, požara ili ljudskih grešaka,

neophodno je redovito izrađivati rezervne kopije svih podataka važnih za održavanje vitalnih funkcija informacijskog sustava i sklopovlja.

Prethodni stavak prvenstveno se odnosi na kopije sustava središnjih poslužitelja, knjižničkog poslužitelja, računovodstvenih podataka i podataka o konfiguraciji softvera neophodnog za funkcioniranje mreže.

Članak 19.

Za izradu rezervnih kopija podataka središnjih poslužitelja, rezervnih kopija podataka važnih za održavanje vitalnih mrežnih funkcija i računala važnih za podršku korisnicima te za neprekidnost rada poslužitelja nadležan je davatelj usluge na Fakultetu.

Članak 20.

Fakultet je dužan izraditi zaseban dokument u kojem se definiraju procedure za izradu rezervnih kopija, imenuju odgovorne osobe, određuje potrebna oprema, te prostor za čuvanje kopija.

Radi osiguranja neprekinutosti poslovanja, Fakultet je dužan razraditi procedure za oporavak kritičnih sustava te ih čuvati u pismenom obliku, kako bi u slučaju zamjene izvršitelja novozaposleni djelatnici mogli brzo reagirati u slučaju nesreće. Dokumentaciju čuva voditelj sigurnosti.

Nadzor nad informacijskim sustavima

Članak 21.

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 Opće uredbe o zaštiti podataka i sigurnosnim standardima.

Nadzor smiju obavljati samo osobe koje je Fakultet za to ovlastio.

Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. No u slučaju da je korisnik prekršio pravila sigurnosnih standarda, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi, te se one mogu koristiti u stegovnom ili sudskom postupku.

Članak 22.

Korisnici su dužni 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.

Isto vrijedi i za administratore računala i pojedinih servisa, koji su dužni osobama zaduženim za nadzor pomagati pri istrazi. 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,
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Fakulteta.

Članak 23.

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu uskratiti prava korištenja CARNetove mreže i njezinih servisa.

Korištenje računalne opreme Fakulteta

Članak 24.

Nedopuštenim se smatra svako korištenje računala na način koji bi doveo do povrede važećih propisa ili etičkih normi.

Lakšim oblicima nedopuštenog korištenja računala i opreme smatra se:

- ograničena uporaba nelicenciranog softvera,
- skidanje (download) autorski zaštićenih datoteka bez plaćanja naknade ako su iste javno dostupne,
- skidanje (download) i(ili) distribucija sadržaja koji nije primjeren akademskoj zajednici (pornografija i sl.),
- slanje masovnih poruka, bile one komercijalne prirode ili ne, čime se nepotrebno troše mrežni resursi,
- samovoljna instalacija softvera,
- korištenje neprihvatljivih aplikacija i servisa zbog kojih se narušava sigurnost informacijskih sustava, nepotrebno troše mrežni resursi ili se nanosi bilo kakva materijalna i(ili) nematerijalna šteta Fakultetu,
- korištenje računala Fakulteta i ostalih informatičkih resursa Fakulteta u svrhe koje nisu u skladu s Etičkim kodeksom Fakulteta.

Težim oblicima nedozvoljenog korištenja računala i opreme smatra se:

- preuzimanje tuđeg identiteta (korištenje opreme s tuđim korisničkim računom, slanje elektroničke pošte pod tuđim imenom i sl.),
- 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,
- vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti.

Članak 25.

Fakultet zadržava pravo procjene prihvatljivog korištenja računala.

Uprava Fakulteta će sankcionirati neprihvatljive oblike korištenja računala na Fakultetu sukladno težini neprihvatljivog korištenja, a na temelju procjene/mišljenja voditelja sigurnosti.

Korisnici informatičkih resursa i opreme dužni su upozoriti upravu Fakulteta na svaki oblik neprihvatljivog ponašanja korisnika, a prvenstveno su dužni svojim primjerom pozitivno utjecati na promicanje prihvatljivog ponašanja ostalih korisnika.

Zaporke

Članak 26.

Svi zaposlenici Fakulteta, suradnici, studenti i polaznici koji u svome radu koriste računala dužni su pridržavati se pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Minimalna dužina zaporke mora biti šest znakova. U zaporci treba izmiješati mala i velika slova s brojevima

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava. Korisnik je odgovoran za tajnost svoje zaporke.

Antivirusna zaštita i zaštita od neželjene e-pošte (spama)

Članak 27.

Zaštita od virusa je obavezna, a provode je davatelji usluga na Fakultetu nadležni za pojedini dio

sustava.

Članak 28.

Osobe koje provode protuvirusnu zaštitu dužne su instalirati protuvirusne programe na sva korisnička računala i namjestiti ih tako da se izmjene u bazi virusa automatski propagiraju s središnje instalacije ili s vanjskog poslužitelja, bez aktivnog sudjelovanja korisnika.

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ako iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju zatražiti dozvolu od nadležnih davatelja informatičkih usluga.

Članak 29.

Administratori poslužitelja elektroničke pošte dužni su postaviti poslužitelje tako da prilikom primanja poruka konzultira baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje (open relay) te baza s adresama poznatih pošiljatelja neželjene e pošte «spamera». Pošta koja dolazi s tako pronađenih adresa neće se primati.

Rješavanje sigurnosnih incidenata

Članak 30.

Svaki zaposlenik, suradnik, student ili polaznik Fakulteta dužan je prijavljivati sigurnosne incidente, gubitka ili neovlaštene izmjene podataka, pojave virusa i sl.

Voditelj sigurnosti treba izraditi i održavati kontakt listu osoba kojima se prijavljuju problemi u radu mreže, mrežnih servisa i mrežne opreme te obrazac za prijavu incidenta. Kontakt listu treba objaviti na internim mrežnim stranicama Fakulteta.

Svaki incident se dokumentira. Obrazac za prijavu incidenta sadrži opis incidenta i poduzete mjere pri rješavanju problema.

Članak 31.

Izvještaji o incidentima smatraju se povjerljivim dokumentima, spremaju se na sigurno mjesto i čuvaju 10 godina, kako bi mogli poslužiti za statističke obrade kojima je cilj ustanoviti najčešće propuste radi njihova sprečavanja, ali isto tako i kao dokazni materijal u eventualnim stegovnim ili sudskim procesima.

Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u.

Članak 32.

Administratori smiju pratiti korisničke procese. Ako sumnjaju da se računalo koristi na nedopušten način, mogu ispisati 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 voditelju sigurnosti, uz poštivanje slijedećih pravila:

- informacijski sustav se čuva u zatečenom stanju, odnosno ne čine se izmjene koje bi otežale ili onemogućile dijagnosticiranje,
- napravi se kopija zatečenog stanja, po mogućnosti, bez izmijene atributa datoteke,
- dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage,
- o istrazi se napiše izvještaj.

Izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na način da im pristup imaju samo ovlaštene osobe.

Fakultet može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih

i osobnih informacija.

Članak 33.

Svrha je istrage da se odredi uzrok nastanka problema te da se iz toga izvuku zaključci o tome kako spriječiti ili se pripremiti za slične situacije. Ako je uzrok sigurnosnom incidentu bio ljudski faktor, protiv odgovornih se mogu poduzeti sankcije.

Fakultet može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili pristup podacima.

Ako je incident izazvao zaposlenik vanjske tvrke ili ustanove, Fakultet može zatražiti od njegovog poslodavca da ga zamijeni te da drugu osobu ovlasti za obavljanje posla na Fakultetu. U slučaju teže povrede pravila sigurnosnih standarda, Fakultet može raskinuti ugovor s vanjskom tvrtkom ili ustanovom.

Završne odredbe

Članak 33.

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

KLASA: 003-05/18-02/0001
URBROJ: 2181-190-00-18-00015
Split, 5. lipnja 2018.

DEKANICA
izv. prof. dr. sc. Gloria Vickov

Ovaj Pravilnik objavljen je na službenim mrežnim stranicama i oglasnoj ploči u sjedištu Filozofskog fakulteta u Splitu dana 5. lipnja 2018. godine te stupa na snagu dana 13. lipnja 2018. godine.

TAJNICA

Maja Kuzmanić, dipl. iur.