SVEUČILIŠTE U SPLITU

FILOZOFSKI FAKULTET

SIGURNOSNA POLITIKA INFORMACIJSKOG SUSTAVA FILOZOFSKOG FAKULTETA U SPLITU

Split, studeni 2025. godine

Na temelju članka 31. Statuta Filozofskog fakulteta u Splitu (pročišćeni tekst, prosinac, 2023.) prof. dr. sc. Ina Reić Ercegovac, dekanica Filozofskog fakulteta u Splitu, dana 10. studenog 2025. godine, donosi

Sigurnosnu politika informacijskog sustava Filozofskog fakulteta u Splitu

I. Opće odredbe

Članak 1.

Sigurnosnom politikom informacijskog sustava Filozofskog fakulteta u Splitu (dalje: Sigurnosna politika) reguliraju se skupovi pravila koji propisuju mjere koje moraju biti sadržane u organizacijskom i tehničkom dijelu upravljanja informacijskim sustavom Filozofskog fakulteta u Splitu (dalje: Fakultet).

Članak 2.

(1) Sigurnosna politika dio je sustava upravljanja sigurnošću informacijskih sustava. Njezina je svrha da definira prihvatljive i neprihvatljive načine ponašanja, da jasno raspodijeli zadatke i odgovornosti, te da propiše sankcije u slučaju nepridržavanja.
(2) Fakultet kao ustanova CARNet članica u potpunosti prihvaća CARNet-ov dokument CDA 0035 - Odluka o prihvatljivom korištenju CARNet mreže (https://www.carnet.hr/wp-content/uploads/2019/11/CDA0035.pdf) .

Članak 3.

Pravila rada i ponašanja koja definira sigurnosna politika odnose se na svu računalnu opremu koja se nalazi u prostorima Fakulteta ili je u vlasništvu Fakulteta te je priključena u mrežu Fakulteta, sav instalirani softver i sve mrežne usluge, a obvezna su za:

- administratore informacijskih sustava – davatelje informatičkih usluga
- korisnike (zaposlenici, vanjski suradnici, studenti, polaznici obrazovnih programa te drugi korisnici usluga Fakulteta)
- vanjske dionike (vanjske tvrtke) koji održavaju računalnu opremu ili softver koji se koristi na opremi Fakulteta.

II. Administratori informacijskog sustava – davatelji informatičkih usluga

Članak 4.

(1) Davatelj informatičkih usluga su zaposlenici Fakulteta u Odjelu za administrativnu i informatičku podršku zaduženi za skrb o radu računala i računalne mreže (dalje: IT zaposlenici), a koji su odgovorni za neprekidan rad računalne mreže i nadgledanje rada informacijskog sustava.
(2) IT zaposlenici instaliraju licencirane programe podržane od Ministarstva znanosti, obrazovanja i mladih (dalje: MZOM) ili nabavljene za potrebe Fakulteta.
(3) Korištenje nelicenciranog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva.
(4) Informatički specijalist je dužan brinuti o ukupnoj sigurnosti svih informacijskih sustava koji su u njegovoj nadležnosti te sigurnosnih kopija podataka kojima ima pristup, a što uključuje i fizičku sigurnost poslužiteljske računalne opreme.

Administriranje računala

Članak 5.

(1) IT zaposlenici dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke.

(2) U slučaju da drugi zaposlenici žele samostalno administrirati osobno računalo na kojem rade, moraju potpisati izjavu o preuzimanju odgovornosti za administriranje računala.

(3) Računala trebaju biti konfigurirana na način da budu zaštićena od potencijalnih napada „izvana" i „iznutra" instaliranjem dodatnog softvera, listama pristupa, filtriranjem prometa, konfiguracijama mrežnih preklopnika te na druge načine prikladne načine, na prijedlog informatičkog specijaliste, a sukladno preporukama struke.

(4) Posebnu pozornost IT zaposlenici će posvetiti onoj opremi kojom se obavljaju ključne funkcije na Fakultetu ili koja sadrži povjerljive informacije koje treba štititi od neovlaštenog pristupa.

(5) IT zaposlenici svakodnevno prate rad sustava i provjeravaju rad usluga, a u svom radu dužni su poštivati povjerljivost informacija s kojima pri obavljanju poslova dolaze u dodir.

(6) U slučaju potrebe više istovremenih poslova na sustavu, prioritet određuje informatički specijalist.

Upravljanje mrežom

Članak 6.

(1) IT zaposlenik zadužen za upravljanje mrežom treba imati ažurirane i potpune podatke o svim mrežnim priključcima i umreženim uređajima, uključujući prijenosna računala i druge uređaje koji se spajaju na mrežu Fakulteta.

(2) Bežična mreža Fakulteta osigurana je od mogućnosti priključivanja na privatnu mrežu i snimanja mrežnog prometa te konfigurirana na način da je osigurana međusobna izolacija mrežnih klijenata.

Članak 7.

U slučaju podržavanja rada na daljinu (kada se zaposlenicima dopušta da sa kućnog računala ažuriraju podatke i pristupaju uslugama Fakulteta) zbog mogućnosti da korištenja od strane neautoriziranih osoba mora se osigurati da udaljeno računalo ne ugrozi sigurnost mreže Fakulteta, a povjerljivi podaci na udaljenom računalu moraju biti jednako sigurni kao na računalu u zgradi Fakulteta.

Sigurne zone

Članak 8.

(1) Poslužiteljska računalna i komunikacijska oprema fizički se odvaja u fizički odijeljen prostor - prostor sigurne zone (serverski prostor), u kojem je ulaz dopušten samo IT zaposlenicima koje administriraju mrežnu i komunikacijsku opremu i poslužitelje. Iznimno, po potrebi, ulaz u sigurnu zonu dopušten je i ovlaštenim osobama kao zaposlenicima vanjskih dionika (radi inspekcijskog nadzora, održavanja, neophodnih popravaka i sl.), uz prethodnu najavu informatičkom specijalistu.
(2) Prostor sigurne zone treba biti uredan, čist i klimatiziran, a oprema u sigurnoj zoni treba biti zaštićena od problema s napajanjem električnom energijom te se u njihovoj blizini ne smiju držati zapaljive i eksplozivne stvari.

III. Korisnici informatičkih usluga

Članak 9.

(1) Korisnici 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.
(2) Iznimno, korisnici su odgovorni ako se ne pridržavaju pravila i dužnosti propisanih ovom politikom odnosno ako na neprihvatljiv način koriste računalnu opremu.
(3) Korisnici imaju pravo uporabe odobrenih resursa računala i mreže, a uporaba korisničkog računa kao i sve eventualne druge odobrene usluge su im besplatne.

Članak 10.

Dužnosti korisnika su:

- Pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu sa važećim zakonima, etičkim normama i pravilima lokalne sigurnosne politike.
- Pridržavanja pravila lijepog ponašanja u komunikaciji s drugima na Internetu. Nije dopušteno vrijeđanje i ponižavanje ljudi po vjerskoj, nacionalnoj, spolnoj, rasnoj ili nekoj drugoj osnovi te distribuiranje materijala koji širi mržnju, netrpeljivost, strahove, potiče na nasilje ili je uvredljiv.
- Izbor kvalitetne zaporke i njezina povremena promjena.
- Prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi.
- Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje.
  Vanjski pružatelji usluga osiguravaju automatsku sigurnosnu pohranu (backup) važnih podataka, dok za vlastite podatke i dokumente korisnici moraju od davatelja informatičkih usluga zatražiti uspostavu automatske pohrane važnih informacija, ili u protivnom moraju sami izrađivati sigurnosne kopije.

Članak 11.

Neprihvatljivim korištenjem se smatra svako korištenje računalne opreme na način koji bi doveo do povrede zakona, propisa ili etičkih normi ili na način koji bi mogao izazvati materijalnu ili nematerijalnu štetu za Fakultet, njegove zaposlenike, studente, polaznike i vanjske suradnike, a naročito:

- stvaranje ili prijenos materijala uvredljivog i ponižavajućeg sadržaja;
- stvaranje ili prijenos materijala koji je napravljen da bi izazvao neugodnosti, neprilike ili širio strahove;
- distribuiranje autorski zaštićenih djela bez dozvole vlasnika prava;
- ometanje drugih korisnika u radu odnosno korištenje na način da ometa korištenje drugim korisnicima (preopterećivanjem pristupnih linija ili preklopne opreme);
- širenje, virusa, trojanaca, i ostalog zloćudnog softvera;
- slanje neželjenih masovnih poruka;
- preuzimanje tuđeg identiteta, bilo da se radi o korištenju računala ili servisa pod tuđim imenom, slanje poruka pod tuđim imenom ili kupovini tuđom kreditnom karticom;
- provaljivanje na računala koristeći sigurnosne propuste u softveru;
- traženje sigurnosnih propusta na umreženim računalima bez dozvole vlasnika opreme;
- izvršavanje napada uskraćivanjem resursa (Denial of Service);
- korumpiranje ili uništavanje podataka drugih korisnika;
- povreda privatnosti drugih korisnika;
- uporaba tuđeg korisničkog računa;
- davanje na uporabu svojeg korisničkog računa drugim osobama;

- lažno predstavljanje kroz uporabu mrežnih usluga i servisa;
- uporaba resursa ili podataka koji su dani na privatnu uporabu drugim osobama;
- stavljanje informacija na javnu uporabu putem postojećih mrežnih servisa bez suglasnosti vlasnika informacija;
- uporaba računalnih i mrežnih resursa izvan granica ili na način koji korisniku nije odobren. Ukoliko nije siguran glede prava i načina uporabe nekog resursa, korisnik je dužan obratiti se IT zaposlenicima;
- uporaba mrežnih usluga i servisa koji su zaštićeni lozinkom ili pisanim upozorenjem vlasnika;
- uporaba mrežnih usluga i servisa mimo pravila njihove uporabe;
- korumpiranje ili uništavanje podataka drugih korisnika;
- provaljivanje na računala koristeći sigurnosne propuste u programima i sustavu;
- masovna distribucija pojedinačnih poruka;
- uporaba korisničkog računa u komercijalne svrhe;
- distribuiranje ili publiciranje informacija koje su suprotne opće prihvaćenim moralnim normama ili narušavaju ugled ili privatnost pojedinca;
- davanje netočnih ili zastarjelih podataka u svrhu ostvarivanja korisničkih prava;
- priključivanje na mrežu računala bez dopuštenja IT zaposlenika.

Članak 12.

Korisniku koji se ne pridržava pravila prihvatljivog korištenja bit će tehničkim mjerama uskraćen pristup mreži, a protiv osoba koje podliježu odredbama općih akata Fakulteta o stegovnoj odgovornosti može se pokrenuti stegovni postupak pod uvjetima propisanim tim općim aktima.

Zaposlenici u nastavi, vanjski suradnici i gosti kao korisnici

Članak 13.

(1) Zaposlenici u nastavi odgovaraju za računalnu opremu koju im je Fakultet dodijelio za rad. Računala imaju instalirane programe koje održavaju IT zaposlenici. IT zaposlenici mogu instalirati ili odobriti samo licencirani ili free software, a samostalno instaliranje programa dopušteno je samo uz prethodno odobrenje IT zaposlenika.
(2) Vanjski suradnici i gosti mogu koristiti mrežu i računala Fakulteta u kraćem vremenskom periodu zbog održavanja nastave, seminara, znanstvenih skupova, tečajeva i slično, a njihov pristup fakultetskoj mreži odobrava informatički specijalist uz suglasnost dekana Fakulteta. Vanjski suradnici i gosti odgovaraju za računalnu opremu koju im je Fakultet dodijelio za rad.
(3) Računala koja nisu vlasništvo Fakulteta korisnici mogu priključiti na lokalnu mrežu Fakulteta isključivo uz prethodno odobrenje IT zaposlenika.

Zaposlenici stručnih službi i Knjižnice Fakulteta kao korisnici

Članak 14.

(1) Računalnu opremu dodijeljenu za rad zaposlenika u stručnim službama i Knjižnici Fakulteta koriste isključivo zaposlenici raspoređeni za rad u tim ustrojstvenim jedinicama Fakulteta.
(2) Računala sa podacima važnim za rad i poslovanje Fakulteta moraju imati sigurnosne kopije podataka.
(3) Računala sa sigurnosnom kopijom i način pohranjivanja rezervnih podataka određuju IT zaposlenici.

Studenti i polaznici kao korisnici

Članak 15.

(1) Studenti i polaznici mogu koristiti računala u učionicama, studentskim učionicama i informatičkim učionicama.
(2) Nije dopušteno spajanje osobnih računala studenata i polaznika na lokalnu mrežu Fakulteta bez prethodnog odobrenja IT zaposlenika.
(3) Računala u informatičkim učionicama ne smiju se koristiti bez prethodnog odobrenja zaposlenika u nastavi ili nazočnosti drugog zaposlenika Fakulteta kao odgovorne osobe.
(4) Računala u učionicama instaliraju i održavaju isključivo IT zaposlenici, u dogovoru sa zaposlenicima u nastavi koji koriste učionice. Zaposlenici u nastavi zahtjev za instalacijom aplikacijskih programa koje će koristiti u učionicama mogu predati osobno ili elektroničkom poštom IT zaposlenicima (it@ffst.hr) minimalno 30 dana prije početka nastave.

IV. Prijava kibernetičkog (sigurnosnog) incidenta

Članak 16.

(1) Kibernetički incident je događaj koji ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost pohranjenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacijski sustavi nude ili kojima omogućuju pristup.
(2) Prijava kibernetičkog incidenta na Fakultetu šalje se na e-mail adresu IT zaposlenika: it@ffst.hr. U prijavi treba navesti datum kada se dogodio incident, opis incidenta, dostupne indikatore kompromitacije te druge dostupne relevantne informacije.
(3) Informatički specijalist zadužen je za utvrđivanje razrađene procedure u incidentnim situacijama, a u slučaju incidenta obavlja istragu te poduzima i predlaže radnje potrebne da se što prije informacijski sustav vrati u stanje redovitog funkcioniranja. IT zaposlenici su dužni pomoći informatičkom specijalistu pri istrazi i uklanjanju problema.
(4) U slučaju potrebe zbog sigurnosnih incidenata Fakultet će koristiti usluge stručnjaka za računalnu sigurnost iz CARNET-a, SRCE-a i drugih ugovornih partnera, a sve uključene strane su dužne poštivati pravila o zaštiti podataka i povjerljivosti informacija.
(5) Incidenti se dokumentiraju kako bi se izbjegli u budućnosti, a ako je incident većih razmjera i uključuje kršenje propisa prijavljuje se obvezno meritornim tijelima.

V. Nadzor nad informacijskim sustavima

Članak 17.

(1) Fakultet zadržava pravo nadzora nad instaliranim softverom, podacima koji su pohranjeni na umreženim računalima te načinom korištenja računala.
(2) Nadzor iz stavka 1. ovog članka se smije provoditi radi:
- osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa;
- provedbe istrage u slučaju sumnje da se dogodio sigurnosni incident;
- provjere usklađenosti informacijskih sustava i načina njihova korištenja sa zakonskim odredbama i zahtjevima Sigurnosne politike.

(3) Nadzor može provoditi samo osobe koje je ovlastio, a prilikom provođenja nadzora ovlaštene osobe dužne su poštivati privatnost korisnika i njihovih podataka.
(4) U slučaju utvrđenog kršenja zakonskih propisa i/ili pravila Sigurnosne politike, nema obveze osiguravanja povjerljivosti informacija otkrivenih u istrazi pa se takve informacije mogu koristiti u stegovnom ili sudskom postupku.

VI. Završne odredbe

Članak 18.

(1) Tumačenje odredbi Sigurnosne politike daje dekan.
(2) Na sva pitanja koja nisu uređena ovom politikom na odgovarajući način primjenjuju se pravila Sigurnosne politike informacijskih sustava za članice CARNeta.
(3) Na temelju odredbi ove politike donijet će se prateći dokumenti kojima se definiraju pravila za pojedina područja rada u svrhu provedbe i osiguranja sigurnosti informacijskog sustava Fakulteta.

Članak 19.

Sigurnosna politika stupa na snagu osmog dana od dana objavljivanja na oglasnoj ploči i službenim mrežnim stranicama Fakulteta.

KLASA: 011-04/25-03/00002
URBROJ: 2181-190-25-00010

DEKANICA

prof. dr. sc. Ina Reić Ercegovac

Sigurnosna politika informacijskog sustava Filozofskog fakulteta u Splitu objavljena je na oglasnoj ploči i mrežnim stranicama Fakulteta dana 11. studenog 2025. godine te stupa na snagu dana 19. studenog 2025. godine.

TAJNICA FAKULTETA

Maja Kuzmanić, dipl. iur.