

Na temelju članka članka 22. Pravilnika Fakulteta zdravstvenih znanosti Sveučilišta u Splitu, Stručno vijeće Fakulteta zdravstvenih znanosti Sveučilišta u Splitu na 11. redovitoj sjednici u akademskoj godini 2025./2026., održanoj 22. rujna 2026. donosi

PRAVILNIK O KIBERNETIČKOJ SIGURNOSTI I SIGURNOM KORIŠTENJU INFORMACIJSKIH SUSTAVA FAKULTETA ZDRAVSTVENIH ZNANOSTI

I. OPĆE ODREDBE

Predmet Pravilnika

Članak 1.

- (1) Ovim Pravilnikom uređuju se osnovna pravila i odgovornosti za sigurno korištenje informacijskih sustava, računalne i komunikacijske opreme, korisničkih računa, podataka i digitalnih usluga kojima se koristi Fakultet zdravstvenih znanosti Sveučilišta u Splitu (u daljnjem tekstu: Fakultet).
- (2) Cilj Pravilnika je smanjiti rizik od neovlaštenog pristupa, gubitka ili zlouporabe podataka, zlonamjernih programa, kibernetičkih napada i drugih događaja koji mogu ugroziti poslovanje Fakulteta.
- (3) Odredbe ovog Pravilnika primjenjuju se u skladu s propisima Republike Hrvatske, aktima Sveučilišta u Splitu te pravilima i zahtjevima nadležnih tijela i pružatelja informacijskih usluga.

Područje primjene

Članak 2.

- (1) Ovaj Pravilnik primjenjuje se na sve zaposlenike Fakulteta te, u odgovarajućem dijelu, na vanjske suradnike, studente i druge osobe kojima je omogućen pristup informacijskim sustavima ili opremi Fakulteta.
- (2) Informacijskim sustavima u smislu ovog Pravilnika smatraju se svi informacijski i komunikacijski sustavi i usluge koje Fakultet koristi u svom radu, uključujući sustave Sveučilišta i nacionalne informacijske sustave kojima zaposlenici pristupaju u okviru svojih ovlasti.

II. ODGOVORNOSTI

Odgovornost za kibernetičku sigurnost

Članak 3.

- (1) Dekan osigurava organizacijske uvjete za provedbu mjera kibernetičke sigurnosti na Fakultetu.
- (2) Ustrojstvena jedinica nadležna za informatičko-računarske poslove provodi tehničke i organizacijske mjere zaštite informacijskih sustava u okviru nadležnosti Fakulteta, upravlja korisničkim pristupima za sustave kojima Fakultet upravlja te koordinira postupanje u slučaju sigurnosnog incidenta.
- (3) Čelnici ustrojstvenih jedinica dužni su pravodobno obavještavati nadležnu ustrojstvenu jedinicu o potrebi dodjele, promjene ili ukidanja korisničkih prava.
- (4) Svaki korisnik informacijskog sustava odgovoran je za sigurno korištenje dodijeljenih korisničkih računa, opreme i podataka.

III. KORISNIČKI RAČUNI I PRISTUP SUSTAVIMA

Korisnički računi Članak 4.

- (1) Korisnički račun dodjeljuje se isključivo osobi kojoj je potreban za obavljanje poslova ili drugih odobrenih aktivnosti.
- (2) Korisnički računi i lozinke su osobni i ne smiju se ustupati drugim osobama.
- (3) Korisnici su dužni koristiti sigurnu i jedinstvenu lozinku odnosno zaporku te, kada sustav to omogućuje ili zahtijeva, višefaktorsku autentifikaciju.
- (4) Zabranjeno je čuvanje lozinki na vidljivim ili nezaštićenim mjestima.
- (5) Prava pristupa dodjeljuju se prema načelu najmanjih potrebnih ovlasti, odnosno samo u opsegu potrebnom za obavljanje poslova korisnika.

Promjena i ukidanje korisničkih prava Članak 5.

- (1) Prava pristupa informacijskim sustavima moraju se promijeniti kada zaposlenik promijeni radno mjesto, poslove ili ovlasti.
- (2) Po prestanku radnog odnosa ili drugog temelja za korištenje sustava, pristup se ukida bez nepotrebnog odgađanja.
- (3) Korisnička prava provjeravaju se periodično te se ukidaju prava koja više nisu potrebna.

IV. RAČUNALNA OPREMA I PROGRAMSKA PODRŠKA

Korištenje službene opreme Članak 6.

- (1) Službena računalna i komunikacijska oprema prvenstveno je namijenjena obavljanju poslova Fakulteta.
- (2) Korisnik je dužan službenu opremu štiti od gubitka, krađe, neovlaštenog korištenja i fizičkog oštećenja.
- (3) Na službenu opremu nije dopušteno samostalno instalirati neovlaštenu, nelicenciranu ili sigurnosno nepouzdanu programsku podršku.
- (4) Sigurnosna ažuriranja operacijskih sustava, aplikacija i zaštitnih programa moraju se provoditi redovito.
- (5) Priključivanje privatnih uređaja na informacijsku infrastrukturu Fakulteta dopušteno je samo ako se time ne ugrožava sigurnost sustava i u skladu s pravilima Fakulteta odnosno Sveučilišta.

V. ELEKTRONIČKA POŠTA I INTERNET

Sigurno korištenje elektroničke pošte i interneta Članak 7.

- (1) Korisnici su dužni s posebnom pažnjom postupati s porukama, poveznicama i privicima nepoznatog ili sumnjivog podrijetla.
- (2) Zabranjeno je putem službenih korisničkih računa otvarati sadržaje, pokretati programe ili dostavljati podatke ako postoji sumnja na prijevare, krađu identiteta, zlonamjerni program ili drugu kibernetičku prijetnju.
- (3) Službene korisničke račune nije dopušteno koristiti za registraciju na uslugama koje nisu povezane s poslovnim ili nastavnim aktivnostima Fakulteta ako takva uporaba može povećati sigurnosni rizik.

- (4) Sumnjivu elektroničku poruku ili drugi sigurnosno sumnjiv događaj korisnik je dužan prijaviti nadležnoj ustrojstvenoj jedinici.

VI. ZAŠTITA I POHRANA PODATAKA

Postupanje s podacima Članak 8.

- (1) Podaci kojima Fakultet raspolaže koriste se samo u svrhu za koju su prikupljeni odnosno u okviru službenih ovlasti korisnika.
- (2) Osobni, povjerljivi i drugi zaštićeni podaci ne smiju se bez odobrenja:
- dostavljati neovlaštenim osobama,
 - pohranjivati u privatnim korisničkim računima elektroničke pošte,
 - pohranjivati u neodobrenim uslugama u oblaku,
 - prenositi na nezaštićene prijenosne medije niti
 - iznositi iz informacijskih sustava Fakulteta ako to nije potrebno za obavljanje službenih poslova.
- (3) Dokumentacija koja sadrži osobne ili druge zaštićene podatke mora se čuvati tako da nije dostupna neovlaštenim osobama.

Sigurnosne kopije Članak 9.

Za podatke i informacijske sustave kojima Fakultet samostalno upravlja osigurava se izrada sigurnosnih kopija u skladu s procijenjenim rizikom i važnošću podataka te se, kada je potrebno, provjerava mogućnost njihove obnove.

VII. RAD IZVAN PROSTORA FAKULTETA

Udaljeni pristup Članak 10.

- (1) Pri radu izvan prostora Fakulteta korisnik je dužan poduzeti jednake mjere zaštite podataka i informacijskih sustava kao i pri radu u prostorima Fakulteta.
- (2) Službena oprema ne smije se ostavljati bez nadzora na način koji omogućuje neovlašten pristup.
- (3) Pri korištenju javnih ili drugih nepouzdatih mreža korisnik je dužan posebno voditi računa o zaštiti službenih podataka i pristupnih podataka.

VIII. KIBERNETIČKI SIGURNOSNI INCIDENTI

Prijava incidenta Članak 11.

- (1) Svaki korisnik dužan je bez odgode prijaviti događaj koji može predstavljati kibernetički sigurnosni incident.
- (2) Incidentom se osobito smatra:
- sumnja na neovlašten pristup korisničkom računu ili informacijskom sustavu,
 - gubitak ili krađa službenog računala, mobilnog uređaja ili drugog nosača podataka,
 - primitak ili aktiviranje zlonamjernog sadržaja,
 - neovlašteno otkrivanje, promjena ili brisanje podataka,

- neuobičajeno ponašanje informacijskog sustava,
- sumnja na krađu lozinke ili identiteta te
- svaki drugi događaj koji može ugroziti povjerljivost, cjelovitost ili dostupnost podataka i sustava.

(3) Incident se prijavljuje ustrojstvenoj jedinici nadležnoj za informatičko-računarske poslove, a ako incident uključuje osobne podatke, obavještava se i službenik za zaštitu osobnih podataka u skladu s propisanim postupkom.

(4) Nadležna ustrojstvena jedinica procjenjuje incident, poduzima mjere iz svoje nadležnosti te prema potrebi koordinira postupanje sa Sveučilištem, CARNET-om, pružateljima informacijskih sustava i drugim nadležnim tijelima.

IX. VANJSKI PRUŽATELJI USLUGA

Sigurnost vanjskih usluga Članak 12.

Prilikom nabave ili korištenja informacijskih sustava, računalnih usluga i usluga u oblaku potrebno je, razmjerno važnosti sustava i podataka koji se obrađuju, uzeti u obzir zahtjeve kibernetičke sigurnosti, zaštite podataka, upravljanja korisničkim pristupima, izrade sigurnosnih kopija i dostupnosti podataka.

X. PODIZANJE SVIJEСТИ I PROVJERA SIGURNOSTI

Edukacija korisnika Članak 13.

(1) Fakultet potiče redovito informiranje i edukaciju zaposlenika o kibernetičkoj sigurnosti.

(2) Zaposlenici su dužni upoznati se s pravilima sigurnog korištenja informacijskih sustava i postupati prema sigurnosnim upozorenjima i uputama nadležnih službi.

(3) Fakultet može provoditi periodične provjere sigurnosnih mjera i procjenu kibernetičkih rizika.

XI. POSTUPANJE U SLUČAJU NEPRIDRŽAVANJA PRAVILA

Nepridržavanje sigurnosnih pravila Članak 14.

(1) Ako korisnik postupi protivno ovom Pravilniku i time ugrožava sigurnost informacijskog sustava, mogu mu se privremeno ograničiti ili ukinuti pojedina korisnička prava radi zaštite sustava i podataka.

(2) Ako postupanje predstavlja povredu radne ili druge obveze, odgovornost se utvrđuje prema važećim propisima i općim aktima Sveučilišta i Fakulteta.

XII. ZAVRŠNE ODREDBE

Odnos prema drugim pravilima Članak 15.

Ako su pojedina pitanja kibernetičke sigurnosti uređena propisom, aktom Sveučilišta u Splitu ili obvezujućim pravilima informacijskog sustava na stroži način od ovog Pravilnika, primjenjuju se stroža pravila.

Uputa za kibernetičku sigurnost Članak 16.

- (1) Uputa zaposlenicima za kibernetičku sigurnost nalazi se u Prilogu 1. ovoga Pravilnika i čini njegov sastavni dio.
- (2) Zaposlenici i drugi korisnici informacijskih sustava Fakulteta dužni su postupati u skladu s Uputom iz stavka 1. ovoga članka.
- (3) Uputa sadrži osnovna pravila sigurnog korištenja korisničkih računa, elektroničke pošte, računalne opreme, službenih podataka i informacijskih sustava te pravila prijave sigurnosnih događaja i incidenata.

Stupanje na snagu Članak 17.

Ovaj Pravilnik stupa na snagu osmoga dana od dana objave na mrežnoj stranici Fakulteta, odnosno na drugi način utvrđen općim aktima Sveučilišta i Fakulteta.



Dekan Fakulteta

doc. dr. sc. Mario Podrug

KLASA: 029-03/25-05/06

URBROJ: 2181-228-103/1-200

Split, _____ 2026.

Ovaj Pravilnik objavljen je na mrežnim stranicama i oglasnoj ploči Fakulteta dana
1.10. 2026. godine i stupa na snagu dana
9.10. 2026. godine.

Tajnica Fakulteta

Ljubica Žunić, dipl. iur., univ. spec. iur.

PRILOG 1. – Uputa zaposlenicima za kibernetičku sigurnost: 10 osnovnih pravila sigurnog korištenja informacijskih sustava

**UPUTA ZAPOSLENICIMA ZA KIBERNETIČKU SIGURNOST
10 osnovnih pravila sigurnog korištenja informacijskih sustava**

Radi zaštite podataka, korisničkih računa i informacijskih sustava Fakulteta zdravstvenih znanosti Sveučilišta u Splitu, svi zaposlenici dužni su pridržavati se sljedećih pravila:

1. Čuvajte svoje korisničke podatke

Korisničko ime i lozinka osobni su podaci za pristup sustavima i ne smiju se dijeliti s drugim osobama. Koristite različite i dovoljno složene lozinke te višefaktorsku autentifikaciju (MFA) kada je dostupna.

2. Provjerite poruku prije otvaranja poveznice ili privitka

Budite posebno oprezni s neočekivanim porukama, zahtjevima za unos lozinke, promjenu računa za plaćanje, hitnim zahtjevima ili porukama koje sadrže neuobičajene poveznice i privitke. Ako niste sigurni, ne otvarajte sadržaj i provjerite pošiljatelja drugim komunikacijskim kanalom.

3. Ne unosite lozinku preko poveznice iz sumnjive poruke

Prije prijave provjerite mrežnu adresu stranice. Ako postoji sumnja da je riječ o lažnoj stranici, zatvorite je i pristupite sustavu na uobičajeni način.

4. Zaključajte računalo kada se udaljavate

Čak i pri kratkom napuštanju radnog mjesta zaključajte računalo. Ne ostavljajte dokumente, studentske podatke ili druge povjerljive informacije dostupnima neovlaštenim osobama.

5. Službene podatke čuvajte samo na odobrenim mjestima

Osobne, studentske, kadrovske, financijske i druge službene podatke ne šalžite na privatne adrese elektroničke pošte i ne pohranjujte ih u privatne ili neodobrene servise u oblaku.

6. Ne instalirajte programe bez potrebe i odobrenja

Na službena računala ne instalirajte neprovjerene, nelicencirane ili privatne programe i dodatke koji nisu potrebni za obavljanje poslova.

7. Redovito ažurirajte uređaje

Ne odgađajte sigurnosna ažuriranja operacijskog sustava, preglednika i drugih aplikacija. Ažuriranja uklanjaju poznate sigurnosne ranjivosti.

8. Oprezno koristite USB uređaje i vanjske medije

Ne priključujte nepoznate USB uređaje i druge prijenosne medije na službena računala. Podatke koji sadrže osobne ili povjerljive informacije ne prenosite na nezaštićenim uređajima.

9. Posebno pazite pri radu izvan Fakulteta

Službeno računalo i dokumentaciju čuvajte od krađe i neovlaštenog pristupa. Pri korištenju javnih Wi-Fi mreža izbjegavajte pristup osjetljivim sustavima ako nije osigurana odgovarajuća zaštita.

10. Svaki sumnjivi događaj odmah prijavite

Odmah prijavite:

- sumnjivu elektroničku poruku ili pokušaj krađe lozinke,
- slučajno otkrivanje ili slanje podataka pogrešnoj osobi,
- gubitak ili krađu službenog uređaja,
- sumnju da je netko pristupio vašem korisničkom računu,
- pojavu zlonamjernog programa ili neuobičajeno ponašanje računala.

Ne pokušavajte samostalno „popravlјati“ sigurnosni incident niti ga prešućivati. Brza prijava može znatno smanјiti posljedice.

Kome prijaviti sumnjivi događaj?

Sigurnosni događaj ili incident prijavlјuje se ustrojstvenoj jedinici Fakulteta nadležnoj za informatičko-računarske poslove.

Ako događaj uključuje osobne podatke, prema potrebi se uključuje i službenik za zaštitu osobnih podataka.

Zapamtite: kibernetička sigurnost nije samo odgovornost informatičke službe. Sigurnost sustava u velikoj mjeri ovisi o svakodnevnom postupanju svakog korisnika.