Na temelju članka 13. Statuta Pravnog fakulteta u Rijeci (u daljnjem tekstu: Fakultet), donosi se

POLITIKA INFORMACIJSKE SIGURNOSTI

PRAVNOG FAKULTETA U RIJECI

1. OPĆE ODREDBE

Članak 1.

(1) Politikom informacijske sigurnosti Fakulteta (u daljnjem tekstu: Politika) uspostavlja se okvir politika za upravljanje informacijskom sigurnosti Fakulteta, u sklopu kojeg se određuju ciljevi informacijske sigurnosti, mjere upravljanja sigurnosnim rizicima, organizacijski sustav i raspodjela uloga, odgovornosti i obveza te procesi upravljanja informacijskom sigurnosti.

(2) Pojmovi u ovoj Politici tumače se u skladu s odredbama Zakona o kibernetičkoj sigurnosti (NN 14/24), Zakona o informacijskoj sigurnosti (NN 79/07 i 14/24), Zakona o tajnosti podataka (NN 79/07 i 86/12), Uredbe o kibernetičkoj sigurnosti (NN 135/24) i drugih primjenjivih propisa.

(3) Izrazi koji se koriste u ovoj Politici, a imaju rodno značenje jednako se odnose na muški i ženski rod.

Članak 2.

(1) Ova Politika primjenjuje se na sve informacijske sustave Fakulteta, uključujući mrežne i kibernetičke, u okviru cjelokupne djelatnosti Fakulteta te na sljedeće osobe, koje djeluju samostalno ili posredno, putem tehničkih sredstava i sustava koje koriste ili za koje su odgovorne:

- zaposlenike Fakulteta i vanjske suradnike Fakulteta,
- studente Fakulteta i polaznike drugih obrazovnih programa na Fakultetu,
- partnere i dobavljače te
- sve ostale osobe koje pristupaju ili koriste podatke te informacijske sustave Fakulteta, uključujući mrežne i kibernetičke.

(2) Osobe iz stavka 1. ovog članka dužne su poštivati propisane mjere sigurnosti te svojim postupanjem aktivno pridonositi očuvanju, održavanju i unaprjeđenju informacijske sigurnosti Fakulteta.

2. CILJEVI SIGURNOSTI INFORMATIČKIH SUSTAVA

Članak 3.

Kako bi se osigurala sposobnost djelovanja, spriječio gubitak podataka ili šteta te osigurala provedba zakona i drugih propisa o informacijskoj sigurnosti, prvenstveni ciljevi ove Politike su:

- zaštititi informacijsku (programsku i sklopovnu) imovinu Fakulteta,
- zaštititi podatke zaposlenika i studenata Fakulteta, kao i osoba s kojima Fakultet surađuje u skladu s propisima,
- održavati dosljednost u zaštiti povjerljivosti, cjelovitosti i dostupnosti podataka, procesa, aplikacija i komponenti informacijske tehnologije Fakulteta u skladu s propisima,
- procijeniti rizik te predvidjeti i primijeniti mjere zaštite informacijskih sustava i podataka, uključujući u slučaju kibernetičkog incidenta,
- osigurati druge oblike usklađenosti postupanja sa zakonskim, regulatornim i ugovornim obvezama u pogledu informacijske sigurnosti.

3. UPRAVLJANJE INFORMACIJSKOM SIGURNOSTI

Članak 4.

(1) Dekan je odgovoran za donošenje i nadzor provedbe ove Politike.

(2) U provedbi ove Politike dekanu u radu pomažu prodekan i zaposlenik na informatičkim poslovima koje imenuje dekan.

(2) Zaposlenik na informatičkim poslovima iz stavka 2. ovog članka odgovoran je za provedbu tehničkih mjera, praćenje i reagiranje na incidente, održavanje sustava te predlaganje tehničkih ili organizacijskih poboljšanja.

Članak 5.

(1) Uprava Fakulteta zadužena je za kontinuirani razvoj svijesti i kompetencija iz područja informacijske, a osobito kibernetičke sigurnosti u skladu s potrebama Fakulteta.

(2) Fakultet u svrhu iz stavka 1. ovog članka provodi edukacije za zaposlenike i studente ili upućuje zaposlenike na odgovarajuće vanjske edukacije, radi podizanja razine svijesti o sigurnosnim prijetnjama i jačanja otpornosti zaposlenika i studenata na kibernetičke rizike.

4. UPRAVLJANJE RIZICIMA

Članak 6.

(1) Fakultet primjenjuje pristup informacijskoj sigurnosti temeljen na procjeni rizika, poštujući pritom priznate dobre prakse, standarde i smjernice.

(2) Radi smanjenja procijenjenog rizika informacijske sigurnosti, Fakultet poduzima odgovarajuće mjere, vodeći računa o načelima razumnosti, ekonomičnosti i jednostavnosti korištenja te materijalnim i ljudskim resursima koja mu stoje na raspolaganju.

Članak 7.

(1) Prodekan i zaposlenik na informatičkim poslovima iz članka 4. stavka 2. ove Politike određuje i redovito ažurira minimalne standarde mjera informacijske sigurnosti Fakulteta, a po potrebi i više standarde zaštite. Navedeni sigurnosni standardi moraju odražavati suvremenu i priznatu dobru praksu te osigurati odgovarajuću zaštitu podataka, procesa, aplikacija i informacijskih sustava.

(2) Zaposlenik na informatičkim poslovima iz članka 4. stavka 2. ove Politike bez odgode procjenjuje rizik i poduzima potrebne radnje na temelju vlastitih saznanja ili na temelju prijave koju zaprimi na adresu e-pošte webmaster@pravri.uniri.hr.

(3) Ako procijeni da je riječ o riziku kojim nije moguće upravljati primjenom uobičajenih mjera (poput slanja poruke e-pošte ili drugog načina obavještavanja relevantnih osoba odnosno manjom tehničkom prilagodbom), zaposlenik na informatičkim poslovima iz članka 4. stavka 2. ove Politike bez odgode o tome obavještava dekana te u suradnji s njim planira i provodi potrebne mjere.

Članak 8.

(1) Korištenje vanjskih informacijskih usluga na Fakultetu podliježe prethodnom odobrenju na temelju procjene rizika informacijske sigurnosti i potrebe za poduzimanjem sigurnosnih mjera koje daje dekan na temelju mišljenja prodekana i zaposlenika na informatičkim poslovima iz članka 4. stavka 2. ove Politike.

(2) Informacijske usluge koje pruža Sveučilišni računski centar Sveučilišta u Zagrebu te usluge koje su dostupne u sustavu visokog obrazovanja i znanosti kroz nacionalno financiranje Ministarstva znanosti, obrazovanja i mladih kao i druge usporedive usluge u Hrvatskoj i Europskoj uniji, ne podliježu odobrenju iz stavka 1. ovog članka.

Članak 9.

(1) Fakultet upravlja informacijskom sigurnosti pojedinih vrsta podataka, pri čemu se prepoznaju rizici i provode mjere zaštite prema posebnim propisima, internim aktima te standardima i smjernicama.

(2) U pogledu zaštite osobnih podataka u sklopu informacijskih sustava potrebna je suradnja s Povjerenikom za zaštitu osobnih podataka.

(3) Za označavanje povjerljivih podataka u sklopu informacijskih sustava odgovarajućom oznakom razine povjerljivosti te za procjenu rizika i provedbu mjera sigurnosti ovlašten je dekan.

(4) Za podatke ili skupove podataka koji mogu biti predmet zaštite pravom intelektualnog vlasništva provodi se procjena njihovog pravnog statusa te potreba poduzimanja formalnih radnji radi njihove zaštite.

5. TEHNIČKE MJERE ZA PODIZANJE OTPORNOSTI

Članak 10.

Prodekan i zaposlenik na informatičkim poslovima iz članka 4. stavka 2. ove Politike su odgovorni za određivanje, a zaposlenik na informatičkim poslovima iz članka 4. stavka 2. ove Politike i za provedbu nužnih tehničkih i mjera fizičke sigurnosti za podizanje otpornosti, a osobito:

- upravljanje mrežom i mrežnim resursima radi nadzora i ograničavanja pristupa dijelovima mreže,
- mehanizme za izradu i oporavak sustava iz sigurnosnih kopija,
- zaštitu od neželjene elektroničke pošte,
- nadležnosti i postupke namještanja računalne okoline u smislu instalacije operacijskog sustava i sigurnosnih elemenata na računalima i sustavima
- pravila i postupke instalacije računalnih programa,
- sigurnosne postupke i mjere pri instalaciji i konfiguraciji računalnih programa,
- definiranje smjernica za složenost i ažuriranje lozinki te korištenje višefaktorske autentifikacije,
- nadzor mrežnog prometa i dnevničkih zapisa s ciljem rane identifikacije napada.
- ostale potrebne mjere koje proizlaze iz dobre prakse.

Članak 11.

(1) Radi jačanja otpornosti, zaposlenik na informatičkim poslovima iz članka 4. stavka 2. ove Politike će u roku od četiri mjeseca od stupanja na snagu ove Politike sastaviti i podnijeti dekanu u pisanom obliku Izvješće o stanju informacijske sigurnosti i planu mjera informacijske otpornosti Fakulteta koje sadrži najmanje:

- sustavan pregled informacijske sigurnosti i informacijskih sustava Fakulteta,
- popis i sigurnosna obilježja vlastitih informacijskih usluga Fakulteta, informacijskih usluga koje su na raspolaganju kao dio sustava visokog obrazovanja i znanosti te vanjskih informacijskih usluga,
- procjenu rizika informacijske sigurnosti Fakulteta, općenito i po pojedinim elementima,
- sadržaj tehničkih mjera za podizanje informacijske otpornosti Fakulteta (rukovanje zaporkama, pravila izrade sigurnosnih kopija podataka, sigurno korištenje e-pošte i drugih oblika e-komunikacije, obvezu korištenja zaštite od malicioznih programa i neovlaštenog pristupa),
- plan prevencije i rješavanja sigurnosnih incidenata,
- minimalne sigurnosne zahtjeve za vanjske informacijske usluge.

(2) U dijelu u kojem je informacijska sigurnost prema točkama iz stavka 1. ovog članka dostatno osigurana kroz sigurnosne mjere vanjskih informacijskih usluga, u Izvješću o stanju informacijske sigurnosti i planu mjera informacijske otpornosti Fakulteta dovoljno ih je opisati.

(3) Pri izradi Izvješće o informacijskoj sigurnosti i planu mjera informacijske otpornosti Fakulteta uzet će u obzir i Izvješće o digitalnoj zrelosti Pravnog fakulteta u Rijeci od 20. veljače 2026. koje je rezultat sudjelovanja u pilot fazi projekta e-Sveučilišta.

6. ZAVRŠNE ODREDBE

Članak 12.

Ova Politika stupa na snagu danom objave na službenim mrežnim stranicama Fakulteta.

KLASA: 650-02/26-01/3
URBROJ: 140-01-26-2
U Rijeci, 10. ožujka 2026.

D E K A N

prof. dr. sc. Dario Đerđa