Na temelju članka 48. stavka 2. Statuta Pomorskog fakulteta u Splitu, sukladno Strategiji razvoja Pomorskog fakulteta u Splitu za razdoblje 2024.–2030. (točka I.3.5) i Odluci o prihvatljivom korištenju CARNet mreže (CDA-0035, verzija 4.0), na prijedlog Centra za kvalitetu, Fakultetsko vijeće Pomorskog fakulteta u Splitu na svojoj 20. sjednici održanoj 17. studenog 2025. godine donosi

Sigurnosnu politiku
Pomorskog fakulteta u Splitu

1. SVRHA I CILJEVI POLITIKE

Ovom politikom uređuju se mjere zaštite informacijskih sustava Pomorskog fakulteta u Splitu (u daljnjem tekstu: Fakultet), odgovornosti korisnika i postupci u slučaju povrede sigurnosti.

Svrha ove politike je definirati okvir, mjere i odgovornosti kojima se osigurava povjerljivost, cjelovitost i dostupnost informacijskih sustava, podataka i digitalnih resursa Fakulteta.

Sigurnosna politika ima i edukativnu ulogu – podiže svijest korisnika o važnosti zaštite informacija, pravilnom korištenju digitalnih resursa i smanjenju rizika u svakodnevnom radu.

Ciljevi politike su:

- zaštititi povjerljivost, cjelovitost i dostupnost (CIA) podataka i sustava
- smanjiti rizike koji mogu ugroziti poslovanje, nastavu i istraživanje na Fakultetu
- osigurati usklađenost s GDPR-om, ISO/IEC 27001 i 27002, zakonima RH i smjernicama CARNet-a
- definirati jasne odgovornosti, pravila i postupke za sigurnu uporabu informacijskih resursa.

Informacijski resursi Fakulteta su vrijedna imovina i njima se mora upravljati odgovorno, s ciljem osiguravanja zakonite, sigurne i učinkovite uporabe.

2. REFERENCE

1. ISO/IEC 27001:2022 – Information Security Management Systems
2. ISO/IEC 27002:2022 – Code of Practice for Information Security Controls
3. ISO/IEC 27005:2022 – Information Security Risk Management
4. Uredba (EU) 2016/679 (GDPR) – Opća uredba o zaštiti osobnih podataka
5. Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/18)

6. CCERT-PUBDOC-2009-05-265 – Sigurnosna politika informacijskih sustava za članice CARNet-a
7. CARNet CDA-0035 – Odluka o prihvatljivom korištenju CARNet mreže
8. Zakon o visokom obrazovanju i znanstvenoj djelatnosti (NN 119/22)
9. Pravilnik o obradi i zaštiti osobnih podataka Pomorskog fakulteta u Splitu (važeća verzija)
10. Pravilnik o korištenju sustava video nadzora Fakulteta i izmjene (2024.)

3. DEFINICIJE

- **Centralizirani informacijski sustav**i – računalna i mrežna infrastruktura (poslužitelji, *routeri*, preklopnici, pristupne točke) i pripadajući softver koji održava Informacijsko-računalni odjel (u daljnjem tekstu: IT odjel) Fakulteta.
- **Računalna oprema** – sva hardverska oprema korištena za obradu, pohranu ili prijenos podataka Fakulteta.
- **Podaci** – sve informacije, u elektroničkom ili fizičkom obliku, koje se koriste u poslovanju, nastavi i istraživanjima Fakulteta.
- **Decentralizirani sustavi** – sustavi ili baze podataka koje održavaju pojedini zavodi ili katedre, a povezani su na mrežnu infrastrukturu Fakulteta.
- **Informacijski resurs** (IT resurs) – svaki resurs korišten za elektroničku pohranu, obradu ili prijenos podataka: e-pošta, baze podataka, mediji, fotografije, snimke i dr.
- **Računalna učionica** (**Lab**) – skup računala namijenjenih nastavnim ili istraživačkim aktivnostima.
- **Mobilni uređaj** – svaki prijenosni uređaj (laptop, tablet, pametni telefon, USB medij) koji se koristi za pristup podacima Fakulteta.
- **Osjetljivi podaci** – informacije čije bi otkrivanje, izmjena ili gubitak mogli štetiti interesima Fakulteta, studentima, zaposlenicima ili partnerima (osobni, financijski, istraživački podaci).
- **Korisnik** – svaka osoba (zaposlenik, student, suradnik, vanjski partner) koja ima pristup podacima ili sustavima Fakulteta.
- **Sigurnosni incident** – svaka pojava koja narušava ili može narušiti povjerljivost, cjelovitost ili dostupnost informacija ili sustava.
- **Sigurnost** – skup mjera za smanjenje rizika od neovlaštenog pristupa, gubitka ili oštećenja informacijskih resursa.
- **Sigurne zone** – prostori u kojima se nalazi poslužiteljska i mrežna oprema, s kontroliranim fizičkim pristupom i evidencijom ulazaka.

4. OPSEG PRIMJENE

Ova politika obuhvaća sve digitalne i papirnate podatke koje Fakultet održava, obrađuje ili distribuira, uključujući sustave koji sadrže osjetljive informacije (npr. studentske, financijske, istraživačke podatke).

Politika se odnosi na sve osobe koje imaju pristup mreži i podacima Fakulteta, uključujući:

- sve zaposlenike, studente, vanjske suradnike i partnere koji koriste informacijske resurse Fakulteta
- sve informacijske sustave, mrežne resurse, aplikacije, baze podataka i digitalne servise,
- sve uređaje (poslužitelje, računala, mobilne uređaje, prijenosna računala, vanjske medije i mrežnu opremu),
- sve podatke u elektroničkom, papirnatom ili drugom obliku koji se koriste u poslovnim, nastavnim ili istraživačkim procesima Fakulteta.

Politika se odnosi na sve sustave i uređaje u vlasništvu Fakulteta. Ova politika se primjenjuje u skladu s načelima akademske slobode i slobodnog prijenosa znanja, uz obvezu zaštite podataka sukladno zakonskim i etičkim načelima.

5. NAČELA INFORMACIJSKE SIGURNOSTI

Sigurnosna politika Fakulteta počiva na načelima:

- **Povjerljivost**: informacije su dostupne samo ovlaštenim osobama.
- **Cjelovitost**: informacije i sustavi ostaju točni, potpuni i neizmijenjeni.
- **Dostupnost**: sustavi i podaci dostupni su ovlaštenim korisnicima kada su potrebni.
- **Odgovornost i sljedivost**: svaki korisnik je odgovoran za svoje postupke u radu s informacijskim resursima. Svaka aktivnost mora biti evidentirana i pripisana korisniku.
- **Zakonitost** i **usklađenost**: svi postupci moraju biti u skladu s GDPR-om, važećim zakonima i propisima RH te politikama Sveučilišta u Splitu.
- **Upravljanje rizicima** – sigurnosne mjere moraju biti proporcionalne utvrđenim rizicima.

6. PROCJENA I UPRAVLJANJE RIZICIMA

Fakultet će uspostaviti i provoditi *procjenu rizika informacijskih sustava* u skladu sa smjernicama CCERT-PUBDOC-2009-05-265.

Procjena rizika provodit će se postupno, sukladno dostupnim resursima, a cilj je osigurati sustavno prepoznavanje prijetnji i ranjivosti informacijskih sustava Fakulteta te planiranje mjera za njihovo ublažavanje.

Procjena rizika obuhvaća:

- identifikaciju prijetnji i ranjivosti informacijskih sustava
- procjenu vjerojatnosti i utjecaja svakog rizika
- određivanje razine rizika i utvrđivanje prioriteta za otklanjanje rizika
- definiranje i provedbu korektivnih mjera (organizacijskih, tehničkih i proceduralnih).

IT odjel vodi evidenciju prepoznatih rizika i mjera zaštite (Registar rizika), izrađuje godišnje izvješće i predlaže korektivne mjere. Revizija rizika provodi se najmanje jednom godišnje ili nakon značajnih promjena sustava.

Rezultate procjene rizika razmatra Fakultetsko vijeće radi usvajanja preporučenih mjera zaštite.

7. ULOGE I ODGOVORNOSTI

ULOGA	ODGOVORNOSTI
DEKAN	Odobrava i nadzire provedbu politike; donosi odluke o sankcijama i prioritetima sigurnosti.
INFORMACIJSKO-RAČUNALNI ODJEL (IT ODJEL)	Provodi procjenu rizika i izrađuje godišnje izvješće o informacijskog sigurnosti; vodi evidenciju rizika; provodi tehničke i organizacijske mjere zaštite; održava infrastrukturu; upravlja pristupima; izrađuje sigurnosne kopije; vodi evidenciju incidenata; educira korisnike. IT odjel koordinira s CARNet CERT-om i Agencijom za zaštitu osobnih podataka (AZOP) u slučaju većih incidenata.
KORISNICI (ZAPOSLENICI, STUDENTI, VANJSKI SURADNICI I UGOVORENI PARTNERI)	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. Koriste sustave u skladu s ovom politikom, čuvaju povjerljivost podataka, prijavljuju incidente i poštuju propise. Korisnici su odgovorni ako se ne pridržavaju pravila propisanih ovim dokumentom.

8. PRAVILA KORIŠTENJA INFORMACIJSKOG SUSTAVA I MREŽE

8.1. Opća načela korištenja

Korištenje informacijskih resursa PFST-a mora biti u skladu s ovom Politikom, dokumentom CDA-0035 (CARNet), GDPR-om i važećim zakonima RH.

Korisnici **ne smiju**:

- koristiti tuđe račune ili dijeliti svoje vjerodajnice
- pokušavati zaobići sigurnosne mehanizme
- širiti zlonamjerni softver ili neprimjeren sadržaj
- koristiti resurse u komercijalne ili političke svrhe
- ometati rad mreže ili sustava.

Korisnici **su dužni:**

- koristiti snažne lozinke i redovito ih mijenjati
- čuvati vjerodajnice i uređaje
- prijaviti svaki incident IT odjelu (kvar@pfst.hr) odmah, najkasnije u roku od 24 sata
- pohranjivati službene dokumente na mrežne resurse PFST-a ili odobrene cloud sustave.

8.2. Zaposlenici i suradnici

- Odgovorni su za službenu opremu koju im je PFST dodijelio.
- Softver instalira isključivo IT odjel (licencirani ili odobreni „free“ softver).
- Za instalacije u učionicama/laboratorijima zahtjev se šalje na kvar@pfst.hr najmanje 30 dana unaprijed.
- Obvezno poštovati povjerljivost i GDPR pri radu s osobnim podacima.

8.3. Dekanat i stručne službe

- Računala koriste samo ovlašteni djelatnici tih službi.
- Računala koja sadrže ključne poslovne podatke moraju imati aktivnu zaštitu (antivirus, *firewall*) i redovite backup kopija servisa stručnih službi.
- IT odjel definira način i raspored pohrane sigurnosnih kopija.

8.4. Administratori informacijskog sustava – davatelji informatičkih usluga

- Administratori su djelatnici Informatičko računalnog odjela.
- Odgovorni su za neprekidan i siguran rad sustava, tehničke mjere zaštite, licence i nadzor mreže.

- Pristup korisničkim podacima dopušten je samo kada je nužno radi održavanja ili istrage incidenta i mora biti evidentiran.

8.5. Studenti

- Smiju koristiti računala u učionicama i informatičkim laboratorijima isključivo u nastavne i istraživačke svrhe te u prisutnosti nastavnika ili tehničara.
- Nije dopušteno spajanje osobnih uređaja na žičanu mrežu Fakulteta bez prethodnog odobrenja IT službe.
- Bežični pristup internetu dozvoljen je isključivo putem eduroam mreže i osobnih AAI@EduHr vjerodajnica.
- Studenti su obvezni poštovati pravila ponašanja u komunikaciji, zabranjeno je vrijeđanje, širenje netrpeljivosti i korištenje mreže za neakademske svrhe.

8.6. Vanjski suradnici i ugovoreni partneri

- Pristup mreži, računalima ili podacima PFST-a dopušten je samo uz pismeno odobrenje dekana i IT službe.
- Vanjski suradnici, dobavljači i partneri moraju **potpisati Izjavu o povjerljivosti i poštivanju sigurnosne politike** prije početka rada.
- Nakon završetka radnog ili ugovornog odnosa, Kadrovska služba ili ISVU koordinator dužni su u roku od 30 radnih dana deaktivirati korisničke račune i pristupe korisnika. Svi službeni podaci i dokumenti moraju se predati IT odjelu ili sigurno izbrisati s uređaja korisnika, uz nadzor ovlaštenih službi Fakulteta.

8.7. Zlouporaba pristupa, podataka ili položaja

Zlouporabom se smatra svaka aktivnost kojom se svjesno, neovlašteno ili neprimjereno koristi pristup informacijama, sustavima ili povlaštenim ovlastima, uključujući, ali ne ograničavajući se na:

- pristup, pregled, izmjena ili brisanje podataka bez opravdanog poslovnog razloga
- korištenje administratorskih prava izvan odobrenih zadataka
- korištenje povlaštenih informacija u osobne ili komercijalne svrhe
- prosljeđivanje povjerljivih podataka trećim osobama bez odobrenja
- neovlašteno kopiranje, spremanje ili prijenos podataka izvan sustava Fakulteta
- prikrivanje ili neprijavljivanje sigurnosnog incidenta.

Svaka zlouporaba pristupa, podataka ili položaja smatra se **težom povredom službene dužnosti** i može rezultirati:

- trenutačnim oduzimanjem pristupa
- disciplinskim postupkom u skladu s internim aktima PFST-a i Sveučilišta u Splitu
- prijavom nadležnim tijelima u skladu sa Zakonom o kaznenom postupku i GDPR-om.

IT odjel je dužan **voditi evidenciju svih administratorskih aktivnosti** te omogućiti reviziju pristupa na zahtjev dekana.

Korištenje mreže Fakulteta uređeno je dokumentom *CARNet CDA-0035 – Odluka o prihvatljivom korištenju CARNet mreže*, čija su pravila sastavni dio ove politike.

9. UPRAVLJANJE INFORMACIJSKOM IMOVINOM

Svi informacijski resursi Fakulteta evidentiraju se u popisu informacijske imovine.

Podaci se klasificiraju prema stupnju povjerljivosti:

- **Javni podaci** – dostupni svima bez ograničenja
- **Interni podaci** – dostupni unutar Fakulteta
- **Povjerljivi podaci** – dostupni ograničenom broju zaposlenika
- **Osjetljivi osobni podaci** – zaštićeni prema GDPR-u i zakonima RH.

Svaka razina klasifikacije ima definirane mjere zaštite, uključujući enkripciju, kontrolu pristupa i ograničeno dijeljenje.

10. PRISTUP I AUTENTIFIKACIJA

- Korisnički računi otvaraju se isključivo od strane referada/kadrovska/ISVU koordinatora uz odobrenje nadređenog.
- Prijava se obavlja pomoću AAI@EduHr vjerodajnica, a gdje je izvedivo koristi se višefaktorska autentifikacija (MFA).

  MFA se trenutno primjenjuje na administratorskim računima za Microsoft 365 Cloud servise i druge račune zadužene za glavnu administraciju, uz mogućnost proširenja na sve korisnike Fakultetske domene.
- Lozinke moraju biti snažne i mijenjati se najmanje jednom godišnje.
- Po prestanku zaposlenja ili studiranja korisnički račun se deaktivira.
- Korisnici su odgovorni za čuvanje svojih vjerodajnica; dijeljenje korisničkog računa nije dopušteno.
- Pristup povjerljivim podacima dopušten je samo ovlaštenim osobama.

11. FIZIČKA I TEHNIČKA SIGURNOST

Sigurne zone

- Serveri, mrežna i komunikacijska oprema nalaze se u ograničenim područjima informacijske infrastrukture s kontroliranim pristupom.
- IT odjel vodi evidenciju pristupa i posjeta svim prostorima s kritičnom informatičkom opremom te koristi video nadzor radi sprječavanja neovlaštenog pristupa i zaštite opreme.

  Sustav video nadzora koristi se isključivo u sigurnosne svrhe, u skladu s GDPR-om, Zakonom o provedbi Opće uredbe o zaštiti podataka (NN 42/18) i Pravilnikom o korištenju sustava video nadzora Fakulteta.

  Snimke se čuvaju najduže 6 mjeseci i dostupne su samo ovlaštenim osobama IT odjela i dekanu.

Zaštita opreme

- Prostori s poslužiteljima i mrežnom opremom moraju imati mehaničku zaštitu, protupožarnu i toplinsku zaštitu, te neprekidno napajanje (UPS).

Vanjski izvođači i serviseri

- Vanjski izvođači i serviseri mogu pristupiti opremi samo uz prethodno odobrenje dekana i uz pratnju ovlaštene osobe IT odjela.

  Svaki pristup mora biti evidentiran i odobren u pisanom ili elektroničkom obliku.

12. UDALJENI PRISTUP I KORIŠTENJE PRIJENOSNIH UREĐAJA

- Udaljeni pristup dopušten je samo preko službenog VPN sustava Fakulteta i uz autorizaciju IT odjela.
- Bežične mreže (Wi-Fi) moraju biti odvojene od internih podatkovnih mreža.
- Prijenosna i mobilna računala moraju imati instaliran antivirusni program i ažurirane sigurnosne zakrpe.
- Svi službeni uređaji podliježu pravilima korištenja i vodi se evidencija o njihovom preuzimanja i vraćanja.
- Zabranjeno je pohranjivanje povjerljivih podataka na nešifrirane vanjske medije ili neodobrene cloud servise.

13. ZAŠTITA I POHRANA PODATAKA

- Podaci se pohranjuju na sigurnim poslužiteljima Fakulteta ili u odobrenim cloud sustavima uz primjenu enkripcije.
- IT odjel redovito izrađuje sigurnosne kopije i testira mogućnost obnove (*Disaster Recovery Plan*).
- Osobni i osjetljivi podaci obrađuju se isključivo u skladu s GDPR-om i internim aktima o zaštiti osobnih podataka.
- **Svi zaposlenici upoznaju se s pravilima pohrane i zaštite podataka prilikom zapošljavanja.**

14. POSTUPANJE U SLUČAJU SIGURNOSNOG INCIDENTA

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.

U prijavi treba navesti datum kada se dogodio incident, opis incidenta, dostupne indikatore kompromitacije te druge dostupne relevantne informacije.

- Svaki korisnik dužan je odmah prijaviti incident (npr. neovlašten pristup, *malware*, gubitak uređaja, kvar sustava).
- Prijava se vrši putem e-mail adrese kvar@pfst.hr .
- IT odjel vodi evidenciju incidenata, provodi analizu i surađuje s CARNet CERT-om i AZOP-om kada je potrebno.
- Ozbiljniji incidenti prijavljuju se dekanu.
- U slučajevima teške povrede politike, mogu se primijeniti disciplinske i pravne mjere.
- Dokumentacija o incidentima čuva se najmanje 10 godina.

15. UPRAVLJANJE POVJERLJIVIM INFORMACIJAMA

- Povjerljive informacije moraju biti jasno označene, čuvane u zaključanim ormarima ili enkriptiranim sustavima.
- Kopiranje, prijenos i uništavanje povjerljivih informacija mora biti dokumentirano i odobreno od odgovorne osobe.
- Prijenos povjerljivih informacija elektroničkim putem mora biti zaštićen enkripcijom.
- Obveza čuvanja povjerljivosti traje i nakon prestanka radnog odnosa.

16. ODRŽAVANJE I ZAŠTITA SUSTAVA

- Svi sustavi i aplikacije moraju se redovito ažurirati sigurnosnim zakrpama.
- Na svim računalima mora biti instalirana antivirusna i *antispyware* zaštita s automatskim ažuriranjem.
- Softveri moraju biti legalno licencirani; instalacije bez odobrenja IT odjela su zabranjene.
- IT odjel redovito provodi reviziju softverskih licenci i nadzire mrežnu aktivnost radi otkrivanja neovlaštenih instalacija.

17. EDUKACIJA I SVIJEST O SIGURNOSTI

- Novi zaposlenici i studenti prolaze inicijalnu obuku o sigurnosti informacija.
- Edukacija se obnavlja najmanje jednom godišnje te obuhvaća teme poput prepoznavanja *phishing* napada, zaštite lozinki i pravilnog rukovanja podacima.
- Fakultet promiče kulturu sigurnosti kroz interne radionice, digitalne letke i e-tečajeve.
- Edukacija obuhvaća i vanjske suradnike koji imaju pristup sustavima Fakulteta.

18. REVIZIJA, PRAĆENJE I POBOLJŠANJE

- Sigurnosna politika se preispituje najmanje jednom godišnje ili nakon značajnih promjena u informacijskoj infrastrukturi.
- IT odjel provodi unutarnje sigurnosne revizije, testove ranjivosti i planove oporavka.
- Rezultati revizije i testiranja ranjivosti razmatraju se na sjednici Fakultetskog vijeća.

19. POSLJEDICE NEPRIDRŽAVANJA POLITIKE

Kršenje ove politike može rezultirati:

- opomenom i obveznim dodatnim osposobljavanjem
- privremenim ili trajnim ograničenjem pristupa IT resursima
- stegovnim postupkom
- raskidom radnog odnosa ili prijavom nadležnim tijelima

ovisno o težini povrede i šteti nastaloj Fakultetu.

U slučaju ozbiljne povrede politike, Fakultet može incident prijaviti CARNet CERT-u i nadležnim tijelima.

Ova sigurnosna politika stupa na snagu danom usvajanja na Fakultetskom vijeću Pomorskog fakulteta Sveučilišta u Splitu.

Provedba politike obvezna je za sve korisnike informacijskih sustava Fakulteta.

Dekan

Izv. prof. dr. sc. Ivan Peronja