Sveučilište u Zagrebu
Fakultet organizacije i informatike
Pavlinska 2, 42000 Varaždin

www.foi.unizg.hr
ured-dekana@foi.unizg.hr
tel: +385 42 390 800

POLITIKA KIBERNETIČKE SIGURNOSTI

Varaždin, studeni 2025.

Sadržaj

Na temelju članka 53. Statuta Sveučilišta u Zagrebu Fakulteta organizacije i informatike (u daljnjem tekstu: Fakultet), Fakultetsko vijeće Fakulteta, na sjednici održanoj 20. studenoga 2025. godine, donijelo je

POLITIKU KIBERNETIČKE SIGURNOSTI

1. OPĆE ODREDBE

Članak 1.

Politika kibernetičke sigurnosti Sveučilišta u Zagrebu Fakulteta organizacije i informatike (u daljnjem tekstu: Politika) uspostavlja okvir za upravljanje kibernetičkom sigurnošću na Fakultetu kako bi se osigurala usklađenost sa zakonodavstvom, najboljim praksama, industrijskim standardima i drugim primjenjivim zahtjevima.

Članak 2.

Politikom se utvrđuju ciljevi kibernetičke sigurnosti, mjere za upravljanje kibernetičkim sigurnosnim rizicima te odgovornosti za njihovu provedbu, kontrolu i praćenje.

Članak 3.

Ciljevi Politike su osigurati sposobnost djelovanja, spriječiti gubitak podataka ili štetu te provesti zakonske obveze koje se odnose na sigurnost i zaštitu poslovnih procesa, podataka, mrežnih i informacijskih sustava:

- očuvanje dostupnosti, autentičnosti, povjerljivosti i cjelovitosti podataka, procesa, aplikacija i ostalih komponenti mrežnih i informacijskih sustava u skladu sa zahtjevima sigurnosti
- otkrivanje, odgovor i postupanje s incidentima, uključujući njihovo praćenje, evidentiranje i prijavljivanje
- osiguravanje kontinuiteta poslovanja u slučaju incidenata
- procjena rizika i primjena odgovarajućih mjera zaštite poslovnih procesa, podataka te mrežnih i informacijskih sustava
- osiguravanje provedbe drugih mjera iz Zakona o kibernetičkoj sigurnosti (NN 14/24) (u daljnjem tekstu: Zakon) i ostalih primjenjivih propisa.

Članak 4.

Uprava i ustrojstvene jedinice Fakulteta odgovorni su za ostvarivanje ciljeva i mjera kibernetičke sigurnosti sukladno mogućnostima (proračunskim i ljudskim resursima) na temelju preporuka i smjernica koje izdaje Koordinator za kibernetičku sigurnost (u daljnjem tekstu: Koordinator).

Članak 5.

Politika se primjenjuje na cjelokupno poslovanje Fakulteta, uključujući sljedeće pojedince:

- zaposlenike i studente Fakulteta
- polaznike drugih obrazovnih programa, vanjske suradnike i dobavljače
- sve ostale subjekte i tehničke sustave koji pristupaju ili koriste podatke te mrežne i informacijske sustave Fakulteta.

Članak 6.

Fakultet će osigurati implementaciju najbolje prakse kibernetičke sigurnosti u svrhu zaštite svojih poslovnih procesa, podataka, mrežnih i informacijskih sustava. Osobe iz prethodnoga članka Politike dužne su poštivati propisane mjere sigurnosti.

Članak 7.

Pojmovi i termini u Politici tumače se sukladno odredbama Zakona, Zakona o informacijskoj sigurnosti (NN 79/07 i 14/24), Zakona o tajnosti podataka (NN 79/07 i 86/12) i Uredbe o kibernetičkoj sigurnosti (NN 135/24).

2. UPRAVLJANJE KIBERNETIČKOM SIGURNOŠĆU

Članak 8.

(1) Sigurnost poslovnih procesa, podataka te mrežnih i informacijskih sustava upravljačka je odgovornost dekana Fakulteta.
(2) Vlasnik podataka je voditelj poslovnog procesa odgovoran za postupak obrade podataka.
(3) Vlasnik podataka treba se odgovorno ophoditi s podacima.

Članak 9.

Dekan odlukom imenuje koordinatora na temelju stručnih kvalifikacija i prakse u području kibernetičke sigurnosti te će se njegove dužnosti, odgovornosti i ovlasti urediti internim aktom.

Članak 10.

Dekan, po potrebi, može imenovati Povjerenstvo za kibernetičku sigurnost kao potporu koordinatoru.

Članak 11.

(1) Uprava Fakulteta dužna je osigurati uvjete i resurse za kontinuirani razvoj svijesti o informacijskoj i kibernetičkoj sigurnosti.
(2) Fakultet će u tu svrhu provoditi periodičke edukacije, u koje je moguće uključiti i vanjske pružatelje usluga, s ciljem osvješćivanja zaposlenika i studenata o kibernetičkoj sigurnosti, upoznavanjem s relevantnim prijetnjama i podizanjem otpornosti.

3. UPRAVLJANJE RIZICIMA I MJERE KIBERNETIČKE SIGURNOSTI

Članak 12.

Fakultet primjenjuje pristup sigurnosti temeljen na procjeni rizika, poštujući priznate dobre prakse i standarde te će za smanjenje rizika na prihvatljivu razinu provoditi odgovarajuće mjere, pritom vodeći računa o načelima razumnosti, ekonomičnosti i jednostavnosti korištenja. Pristup će biti usmjeren na poslovne procese, podatke te mrežne i informacijske sustave koji zahtijevaju višu razinu zaštite. Koordinator je odgovoran za upravljanje kibernetičkim sigurnosnim rizicima te predlaže minimalan standard mjera sigurnosti.

4. KLASIFIKACIJA PODATAKA

Članak 13.

(1) Fakultet će, sukladno propisima, usvojiti vlastita pravila o klasifikaciji podataka i upravljanju klasificiranim podacima.
(2) Vlasnici podataka trebaju predložiti status klasifikacije za podatke koje posjeduju uz objašnjenje o zahtjevima, odnosno propisima koji se primjenjuju.
(3) Konačnu odluku o dodjeli statusa klasifikacije donosi dekan na temelju prijedloga vlasnika podataka i koordinatora.
(4) Vlasnici podataka odgovorni su za točnost klasifikacije.

5. TEHNIČKE MJERE ZA PODIZANJE OTPORNOSTI I EKSTERNALIZACIJA PODATAKA

Članak 14.

Ured za informatičku podršku i Centar za informacijske tehnologije će u suradnji s koordinatorom, a sukladno Politici i ostalim aktima Fakulteta, sudjelovati u određivanju i implementaciji nužnih tehničkih i mjera fizičke sigurnosti za podizanje otpornosti kao što su:

- upravljanje mrežom u smislu ograničavanja i nadzora pristupa
- nadzor mrežnog prometa s ciljem ranog otkrivanja napada
- periodičko penetracijsko testiranje kritičnih elemenata mreže i informacijskih sustava
- sustav za izradu i oporavak sigurnosnih kopija
- sustav zaštite od neželjene elektroničke pošte i malicioznih programa
- smjernice za složenost i ažuriranje lozinki i višefaktorsku autentikaciju
- kontrola pristupa server sobama
- ostale mjere kao primjeri dobre prakse.

Članak 15.

(1) Ako se podaci eksternaliziraju (pohranjuju ili obrađuju) kod vanjskih davatelja IKT usluga, to se obavlja na odgovornost vlasnika podataka. Prije eksternalizacije obvezno je provesti procjenu rizika eksternalizacije.
(2) Posebnim internim aktom propisat će se obveze i uvjeti pristupa vanjskih davatelja IKT usluga mrežnim i informacijskim sustavima Fakulteta.
(3) Sveučilišni računski centar (SRCE) Sveučilišta u Zagrebu neće se smatrati vanjskim davateljem usluga obrade podataka u smislu odredaba Politike.
(4) Dekan može, na temelju provedene procjene rizika i preporuke koordinatora, odobriti korištenje vanjskih davatelja IKT usluga uz primjenu prilagođenih sigurnosnih zahtjeva.

6. ZAVRŠNE ODREDBE

Članak 16.

Fakultet će posebnim internim aktima, a na temelju Politike, urediti pitanja:

- dužnosti, odgovornosti i ovlasti koordinatora i ostalih uključenih osoba;
- metodologije provedbe procjene rizika;
- sadržaja mjera za podizanje otpornosti (zaporke, sigurnosne kopije, sigurno korištenje e-pošte, zaštita od malicioznih programa i sl.);
- prijave i rješavanja sigurnosnih incidenata;
- rukovanja klasificiranim i drugim povjerljivim podacima;

- minimalnih sigurnosnih zahtjeva za vanjske davatelje IKT usluga
- stegovne odgovornosti zaposlenika i studenata
- plana kontinuiteta poslovanja u slučaju incidenata
- izvještavanja i načina komunikacije za vrijeme značajnih incidenata
- minimalnih standarda fizičke sigurnosti za prostorije u kojima se obrađuju ili pohranjuju klasificirani podaci
- ostala pitanja iz domene kibernetičke sigurnosti sukladno Zakonu i ostalim primjenjivim propisima.

Članak 17.

Neispunjavanje ili povreda mjera kibernetičke sigurnosti koje proizlaze iz Politike ili akata Fakulteta i postupaka usvojenih na temelju Politike predstavlja povredu obveza iz radnog odnosa sukladno Pravilniku o radu Fakulteta i može dovesti do stegovne, prekršajne, kaznene i/ili građanske odgovornosti.

Članak 18.

Politiku je potrebno revidirati najmanje jednom godišnje ili ranije u slučaju većih izmjena zakonodavnih propisa, organizacijske strukture ili identificiranih rizika.

Članak 19.

Politika stupa na snagu danom objave na službenim web stranicama Fakulteta.

KLASA: 602-04/25-06/1
URBROJ: 2186-62-14-25-107
U Varaždinu 20. studenoga 2025.

DEKANICA

prof. dr. sc. Marina Klačmer Čalopa