Broj: 01-3-34-5595/26
Sarajevo, 05. 6. 2026. godine

Na osnovu člana 19. Odluke o osnivanju Javne ustanove Institut za razvoj preduniverzitetskog obrazovanja Kantona Sarajevo („Službene novine Kantona Sarajevo", broj 37/21) i člana 27a. stav (4) tačka k) Pravila Javne ustanove Institut za razvoj preduniverzitetskog obrazovanja Kantona Sarajevo, broj: 30/22 od 16. 3. 2022. godine i broj: 01-1-02-9635/24 od 26. 12. 2024. godine, a u vezi s članom 27. Zakona o zaštiti ličnih podataka Bosne i Hercegovine ("Službeni glasnik BiH", br. 12/2025) i Odlukom o donošenju Plana za razvoj finansijskog upravljanja i kontrole za 2026. godinu, broj: 01-3-34-3222/26 od 30. 3. 2026. godine, direktorica JU Institut za razvoj preduniverzitetskog obrazovanja Kantona Sarajevo (u daljem tekstu: Institut) donosi

ODLUKU
O DONOŠENJU SMJERNICA O SIGURNOSTI IT INFRASTRUKTURE

Član 1.

Donose se Smjernice o sigurnosti IT infrastrukture Instituta, koje čine sastavni dio ove Odluke.

Član 2.

Smjernicama iz člana 1. ove Odluke utvrđuju se osnovna pravila, mjere i preporuke za zaštitu informaciono-komunikacione infrastrukture, informacionih sistema, podataka i informacionih resursa Instituta.

Član 3.

Za praćenje primjene Smjernica zadužuje se viši saradnik za IT u Institutu, koji će prema potrebi predlagati unapređenja i izmjene radi jačanja sigurnosti IT infrastrukture Instituta.

Član 4.

Svi radnici Instituta dužni su postupati u skladu sa Smjernicama iz člana 1. ove Odluke.

Član 5.

Ova Odluka stupa na snagu danom donošenja i objavit će se na oglasnoj ploči i na web stranici Instituta.

Direktorica Instituta

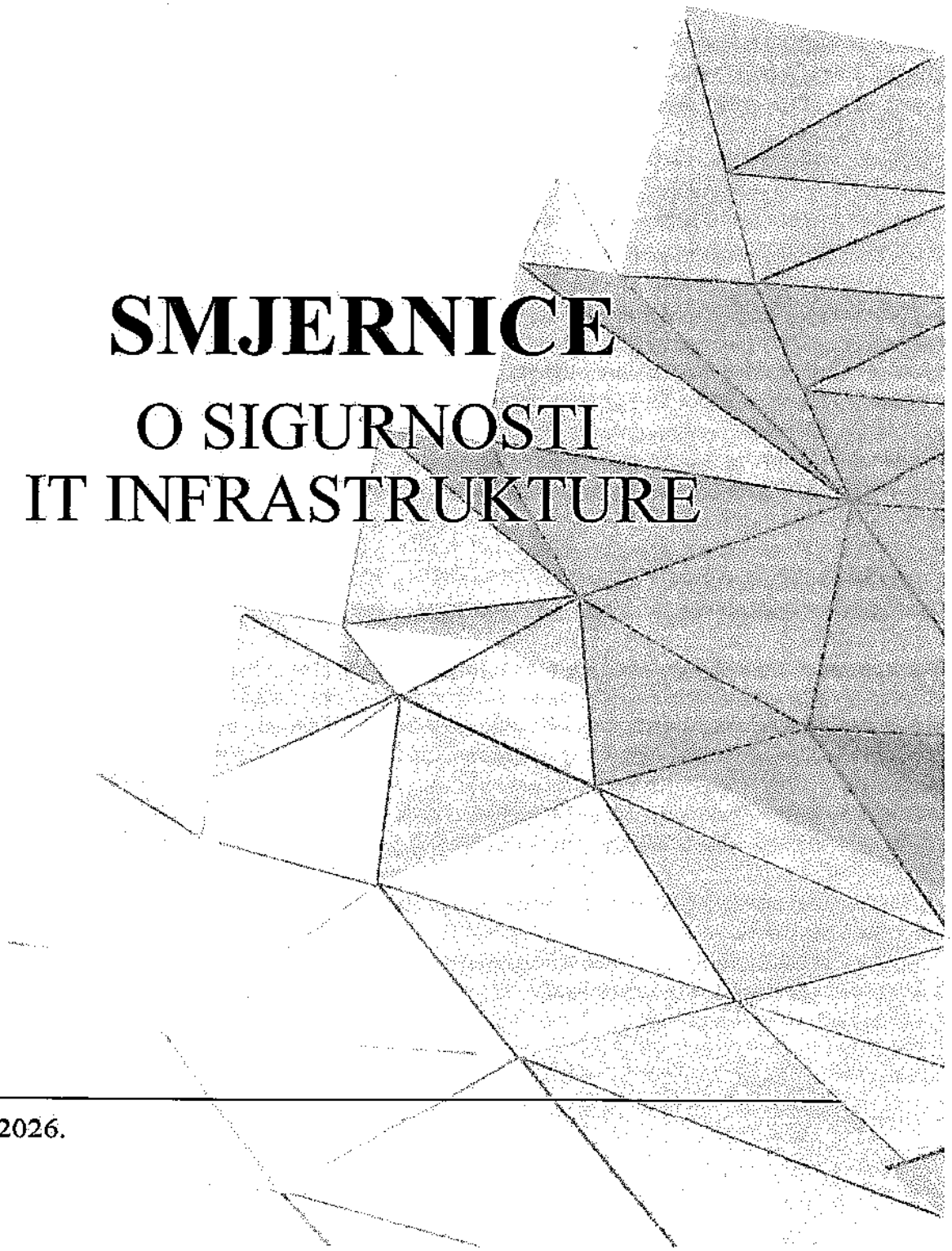
[redacted]

Senada Salihović

Dostavljeno:

1. svim organizacionim jedinicama Instituta;
2. višem saradniku za IT;
3. koordinatoru za FUK;
4. oglasna ploča;
5. web stranica Instituta;
6. a/a.

BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
KANTON SARAJEVO
JU Institut za razvoj preduniverzitetskog obrazovanja
Kantona Sarajevo



SMJERNICE
O SIGURNOSTI IT INFRASTRUKTURE

Sarajevo, juni 2026.

SMJERNICE O SIGURNOSTI IT INFRASTRUKTURE

1. Opće odredbe

Smjernice o sigurnosti IT infrastrukture donose se radi uspostavljanja odgovarajućih kontrola u okviru sistema finansijskog upravljanja i kontrole, a u skladu sa Zakonom o zaštiti ličnih podataka Bosne i Hercegovine, internim aktima Instituta, zahtjevima FUK-a i postojećim IT okruženjem Instituta.

Ovim Smjernicama uređuju se osnovna načela, pravila i odgovornosti u vezi sa zaštitom informacionih resursa, podataka i informaciono-komunikacionih sistema kojima raspolaže JU Institut za razvoj preduniverzitetskog obrazovanja Kantona Sarajevo (u daljem tekstu: Institut).

Smjernice imaju za cilj uspostavljanje odgovarajućeg nivoa zaštite informacija i informacionih sistema, osiguravanje kontinuiteta poslovanja, zaštitu ličnih podataka i drugih podataka kojima Institut raspolaže, te smanjenje rizika od neovlaštenog pristupa, gubitka, izmjene ili uništenja podataka.

2. Cilj smjernica

Ciljevi ovih Smjernica su:

- zaštita povjerljivosti, integriteta i dostupnosti informacija;
- osiguravanje zakonite, sigurne i odgovorne upotrebe informacionih sistema;
- zaštita ličnih podataka i službene dokumentacije;
- uspostavljanje odgovarajućih kontrola pristupa informacionim resursima;
- osiguravanje sigurnosnog kopiranja i oporavka podataka;
- unapređenje svijesti radnika Instituta o informacionoj sigurnosti;
- podrška ostvarivanju ciljeva sistema finansijskog upravljanja i kontrole (FUK).

3. Područje primjene

Ove Smjernice odnose se na sve informacione resurse Instituta, uključujući:

- službene računare i drugu IT opremu;
- službene korisničke naloge i elektronsku poštu;
- mrežne resurse i sisteme za pohranu podataka;
- elektronske baze podataka i evidencije;
- digitalne i elektronske dokumente;
- eksterne medije za pohranu podataka;
- druge informacione i komunikacione sisteme koji se koriste u radu Instituta.

4. Načela informacione sigurnosti

Institut osigurava zaštitu informacionih resursa primjenom načela povjerljivosti, integriteta i dostupnosti informacija.

4.1. Povjerljivost

Povjerljivost podrazumijeva zaštitu informacija od neovlaštenog pristupa, korištenja, otkrivanja ili distribucije.

Institut poduzima odgovarajuće organizacione i tehničke mjere kako bi pristup informacijama bio omogućen isključivo ovlaštenim korisnicima u skladu s njihovim radnim zadacima i dodijeljenim ovlaštenjima.

Radnici Instituta su dužni:

- koristiti isključivo službene korisničke naloge za obavljanje službenih poslova;
- čuvati pristupne podatke i lozinke te ih ne dijeliti s drugim osobama;
- postupati s podacima i dokumentima u skladu s propisima i internim aktima;
- prijaviti svaku sumnju na neovlašten pristup podacima ili informacionim sistemima.

4.2. Integritet

Integritet podrazumijeva očuvanje tačnosti, potpunosti i vjerodostojnosti informacija tokom njihovog kreiranja, obrade, pohrane i korištenja.

Institut osigurava integritet podataka kroz kontrolisane pristupe informacionim sistemima, odgovarajuće procedure arhiviranja i zaštitu informacionih resursa od neovlaštenih izmjena, brisanja ili uništavanja.

Radnici Instituta su dužni:

- unositi i obrađivati podatke tačno i pravovremeno;
- koristiti informacije isključivo u službene svrhe;
- ne vršiti neovlaštene izmjene službenih podataka i evidencija;
- čuvati dokumentaciju i evidencije na način koji omogućava njihovu vjerodostojnost.

4.3. Dostupnost

Dostupnost podrazumijeva osiguravanje pravovremenog i pouzdanog pristupa informacijama i informacionim resursima ovlaštenim korisnicima kada su im potrebni za obavljanje poslova.

Institut osigurava dostupnost podataka kroz korištenje odgovarajućih informacionih sistema, redovno arhiviranje i sigurnosno kopiranje podataka, antivirusnu zaštitu i druge mjere koje doprinose kontinuitetu poslovanja.

U cilju osiguravanja dostupnosti informacija:

- podaci se pohranjuju i arhiviraju na za to predviđenim lokacijama i sistemima;
- provode se mjere zaštite od gubitka podataka i zlonamjernog softvera;
- koriste se sigurnosne kopije podataka radi njihovog oporavka u slučaju incidenta ili tehničkog kvara;
- radnici Instituta su dužni čuvati i koristiti informacione resurse pažljivo i odgovorno.

Sve aktivnosti vezane za obradu, pohranu i korištenje podataka moraju biti usklađene s načelima povjerljivosti, integriteta i dostupnosti informacija.

5. Uloge i odgovornosti

Za provođenje ovih Smjernica odgovorni su rukovodstvo Instituta – direktor Instituta i pomoćnici direktora, viši saradnik za IT – lice zaduženo za administraciju i održavanje informacionih sistema, radnici Instituta, kao i vanjski saradnici angažovani za administraciju i održavanje informaciono-komunikacionih sistema.

Svako lice kojem je odobren pristup informacionim resursima Instituta dužno je koristiti dodijeljena prava pristupa isključivo za potrebe obavljanja poslova iz svoje nadležnosti te postupati odgovorno i u skladu sa pravilima informacione sigurnosti.

5.1. Direktor Instituta

Direktor Instituta odgovoran je za:

- usvajanje i praćenje provođenja Smjernica o sigurnosti IT infrastrukture;
- osiguravanje organizacionih i tehničkih uslova za zaštitu informacionih resursa;
- donošenje odluka o mjerama zaštite informacija i informacionih sistema;
- osiguravanje potrebnih resursa za unapređenje informacione sigurnosti.

5.2. Lica zadužena za administraciju i održavanje informacionih sistema – viši saradnik za IT i vanjski saradnici

Lice zaduženo za administraciju i održavanje informacionih sistema odgovorno je za planiranje, koordinaciju, unapređenje i nadzor nad primjenom mjera informacione sigurnosti u Institutu:

- administrira korisničke naloge, prava pristupa i druge informacione resurse Instituta;
- koordinira aktivnosti antivirusne i sigurnosne zaštite računarske opreme, informacionih sistema i podataka;
- organizira, prati i unapređuje primjenu tehničkih i organizacionih mjera zaštite informacionih resursa;
- koordinira uspostavljanje, održavanje i korištenje sistema za pohranu, arhiviranje i sigurnosno kopiranje podataka;
- prati ispravnost računarske i prateće opreme te koordinira aktivnosti njenog održavanja i servisiranja;
- organizira i prati primjenu internih pravila, preporuka, procedura i uputstava iz oblasti informacione sigurnosti;
- pruža stručnu podršku radnicima Instituta u vezi sa korištenjem informaciono-komunikacionih sistema;
- prati i evidentira sigurnosne incidente te predlaže mjere za njihovo otklanjanje i sprečavanje njihovog ponavljanja;
- daje preporuke za unapređenje digitalnih procesa, informacionih sistema i zaštite podataka;
- prati primjenu ovih Smjernica i predlaže mjere za njihovo unapređenje.

5.3. Rukovodioci organizacionih jedinica – pomoćnici direktora

Rukovodioci organizacionih jedinica odgovorni su za:

- osiguravanje primjene ovih Smjernica u okviru organizacione jedinice kojom rukovode;
- upoznavanje radnici Instituta sa pravilima informacione sigurnosti;
- prijavljivanje uočenih sigurnosnih rizika i incidenata;
- osiguravanje pravilnog upravljanja i arhiviranja dokumentacije iz nadležnosti organizacione jedinice.

5.4. Radnici Instituta

Svi radnici Instituta odgovorni su za:

- korištenje informacionih resursa u skladu sa ~~ovom Politikom~~ ovim Smjernicama i drugim internim aktima;
- zaštitu korisničkih naloga, lozinki i drugih pristupnih podataka;
- čuvanje službenih podataka i dokumentacije od neovlaštenog pristupa, izmjene ili uništenja;
- korištenje službenih e-mail naloga i informacionih resursa u službene svrhe;
- prijavljivanje sigurnosnih incidenata, sumnjivih aktivnosti i drugih događaja koji mogu ugroziti sigurnost informacionih resursa;
- postupanje sa podacima i dokumentacijom u skladu sa propisima koji uređuju zaštitu podataka i kancelarijsko poslovanje.

6. Zaštita ličnih podataka

Institut obrađuje i štiti lične podatke u skladu sa važećim propisima Bosne i Hercegovine koji uređuju oblast zaštite ličnih podataka, kao i drugim relevantnim propisima i internim aktima.

Lični podaci prikupljaju se, obrađuju, koriste, pohranjuju i arhiviraju isključivo u svrhe koje proizlaze iz zakonskih nadležnosti i poslovnih procesa Instituta.

Pristup ličnim podacima dozvoljen je samo ovlaštenim licima kojima su takvi podaci neophodni za izvršavanje poslova iz njihove nadležnosti.

Institut poduzima odgovarajuće organizacione i tehničke mjere radi zaštite ličnih podataka od:

- neovlaštenog pristupa;
- neovlaštene izmjene ili uništenja;
- gubitka podataka;
- slučajnog ili nezakonitog otkrivanja podataka;
- drugih oblika zloupotrebe.

Radnici Instituta koji u okviru svojih poslova imaju pristup ličnim podacima dužni su:

- obrađivati podatke zakonito, pošteno i transparentno;
- koristiti podatke isključivo za potrebe obavljanja službenih poslova;
- čuvati povjerljivost podataka kojima imaju pristup;

- primjenjivati propisane mjere zaštite podataka;
- bez odlaganja prijaviti svaki sigurnosni incident koji može dovesti do povrede zaštite ličnih podataka.

Lični podaci pohranjuju se i arhiviraju na način koji osigurava njihovu povjerljivost, integritet i dostupnost, uz primjenu odgovarajućih kontrola pristupa i mjera zaštite informacionih sistema.

Institut kontinuirano unapređuje mjere zaštite ličnih podataka kroz edukaciju radnika, razvoj internih procedura i primjenu odgovarajućih tehničkih i organizacionih mjera zaštite.

7. Upravljanje korisničkim nalozima i kontrola pristupa

Institut primjenjuje mjere kontrole pristupa kojima se osigurava da informacionim resursima, podacima i sistemima mogu pristupiti isključivo ovlašteni korisnici u okviru svojih nadležnosti i radnih zadataka.

7.1. Korisnički nalozi

Za pristup informacionim resursima Instituta koriste se individualni korisnički nalozi.

Svakom radniku Instituta može biti dodijeljen:

- službeni korisnički nalog za elektronsku poštu i druge servise;
- pristup mrežnim resursima i sistemima za pohranu podataka;
- druga prava pristupa neophodna za obavljanje poslova radnog mjesta.

Korisnički nalozi dodjeljuju se prema principu minimalnih potrebnih ovlaštenja, odnosno korisniku se odobrava samo onaj nivo pristupa koji je neophodan za izvršavanje njegovih radnih zadataka.

7.2. Upravljanje pristupima

Prava pristupa informacionim sistemima dodjeljuju se, mijenjaju i ukidaju u skladu sa poslovnim potrebama Instituta.

Prilikom zasnivanja radnog odnosa ili raspoređivanja na novo radno mjesto korisniku se dodjeljuju odgovarajuća prava pristupa.

U slučaju prestanka radnog odnosa, promjene radnog mjesta ili drugih okolnosti koje utiču na potrebu pristupa informacionim resursima, korisnička prava se mijenjaju ili ukidaju bez odlaganja.

7.3. Korištenje korisničkih naloga i lozinki

Korisnici su odgovorni za korištenje i zaštitu svojih korisničkih naloga i pristupnih podataka.

Zabranjeno je:

- dijeljenje korisničkih naloga i lozinki s drugim licima;

- korištenje tuđih korisničkih naloga;
- omogućavanje neovlaštenim licima pristupa informacionim resursima Instituta.

Korisnici su dužni koristiti lozinke koje pružaju odgovarajući nivo sigurnosti i redovno ih mijenjati kada za to postoji potreba ili sumnja na kompromitaciju pristupnih podataka.

7.4. Pristup podacima i mrežnim resursima

Pristup podacima omogućava se u skladu sa poslovnim potrebama i dodijeljenim ovlaštenjima.

Podaci pohranjeni u sistemima za elektronsku pohranu i arhiviranje dostupni su samo ovlaštenim korisnicima kojima su potrebni za obavljanje poslova iz njihove nadležnosti.

Institut primjenjuje tehničke i organizacione mjere kojima se ograničava pristup podacima, prati korištenje informacionih resursa i smanjuje rizik od neovlaštenog pristupa, izmjene ili gubitka podataka.

8. Tehničke mjere zaštite IT infrastrukture

Radi zaštite podataka i informacionih resursa, Institut primjenjuje odgovarajuće tehničke mjere kojima se osigurava povjerljivost, integritet i dostupnost informacija.

8.1. Službeni korisnički nalozi i elektronska pošta

Svim radnicima Instituta dodjeljuju se službeni korisnički nalozi za elektronsku poštu i korištenje digitalnih servisa Instituta.

Službeni korisnički nalozi uspostavljeni su u okviru Google Workspace okruženja te se koriste za službenu komunikaciju, razmjenu dokumenata i pristup drugim informacionim resursima Instituta.

Radnici su dužni koristiti službene korisničke naloge odgovorno i u skladu sa pravilima informacione sigurnosti.

8.2. Pohrana i sigurnosno kopiranje podataka

Institut osigurava elektronsku pohranu i zaštitu podataka putem sistema za mrežnu pohranu podataka (NAS).

Svim radnicima Instituta omogućen je pristup NAS sistemu radi pohrane i arhiviranja službene dokumentacije i drugih podataka nastalih u procesu rada.

Sigurnosne kopije podataka kreiraju se na NAS sistemu i na eksternim hard diskovima koji su zaduženi po organizacionim jedinicama, u skladu sa potrebama poslovnih procesa.

Radi dodatne zaštite od gubitka podataka, organizacione jedinice koriste eksterne hard diskove koji su zaduženi po sektorima za potrebe kreiranja i čuvanja sigurnosnih kopija podataka.

8.3. Antivirusna zaštita

Svi računari i druga informaciono-komunikaciona oprema koja se koristi u radu Instituta zaštićeni su antivirusnim i sigurnosnim rješenjima. Institut koristi antivirusno i sigurnosno rješenje WithSecure za zaštitu službenih uređaja i podataka.

Antivirusna zaštita instalira se i održava na svim službenim uređajima radi zaštite od zlonamjernog softvera, neovlaštenog pristupa i drugih sigurnosnih prijetnji.

Sigurnosna rješenja redovno se ažuriraju kako bi se osigurao odgovarajući nivo zaštite informacionih resursa.

8.4. Sigurnosni incidenti

Sigurnosnim incidentom smatra se svaki događaj koji može ugroziti povjerljivost, integritet ili dostupnost podataka i informacionih sistema Instituta.

Sigurnosni incidenti uključuju, između ostalog:

- sumnju na neovlašten pristup korisničkom nalogu ili podacima;
- sumnju na kompromitaciju korisničkih lozinki ili korisničkih naloga;
- gubitak ili krađu uređaja;
- pojavu zlonamjernog softvera;
- gubitak, oštećenje ili neovlaštenu izmjenu podataka;
- druge događaje koji mogu ugroziti informacione resurse Instituta.

Radnici Instituta su dužni bez odlaganja prijaviti sigurnosni incident neposrednom rukovodiocu i licu zaduženom za administraciju i održavanje informacionih sistema, a ukoliko incident uključuje ili može uključivati povredu zaštite ličnih podataka, o tome se bez odlaganja obavještava direktor Instituta.

Po prijavi incidenta poduzimaju se odgovarajuće mjere radi ograničavanja posljedica, zaštite podataka, utvrđivanja uzroka i uspostavljanja redovnog funkcionisanja informacionih sistema.

Za koordinaciju aktivnosti vezanih za upravljanje korisničkim nalozima, antivirusnu zaštitu, sigurnosno kopiranje podataka, održavanje informaciono-komunikacione opreme i postupanje u slučaju sigurnosnih incidenata zaduženo je lice zaduženo za administraciju i održavanje informacionih sistema, u saradnji sa rukovodstvom Instituta i drugim radnicima Instituta.

Direktorica Instituta

[redacted]

Senada Salihović