

INSTITUT ZA ISTRAŽIVANJE MIGRACIJA
Trg Stjepana Radića 3, Zagreb

PO LITIKA SIGURNOSTI INFORMACIJSKOG SUSTAVA

Zagreb, rujan 2026.

Na temelju članka 30. Statuta Instituta za istraživanje migracija od 13. prosinca 2023. godine, a u skladu s točkom 1. Odluke o prihvatljivom korištenju CARNet mreže (klasa: 500-200/12/95, ur. broj: I10082-650-109-12-1, verzija 4.0 od 15. lipnja 2012. godine), Upravno vijeće Instituta za istraživanje migracija na 37. sjednici održanoj 22. rujna 2026. godine donijelo je

POLITIKU SIGURNOSTI INFORMACIJSKOG SUSTAVA

Članak 1.

- (1) Ovaj dokument ima za cilj definirati načela i strategiju programa sigurnosti informacijskog sustava (dalje u tekstu: politika sigurnosti) Instituta za istraživanje migracija (u daljnjem tekstu: Institut).
- (2) Pojmovi koji se u ovoj Politici navode u muškom rodu neutralni su i odnose se jednako na osobe muškoga i ženskoga spola.
- (3) Informacijski sustav mora omogućiti neometano odvijanje poslovnih procesa kroz upotrebu informacija. Obavljanje poslovnih procesa Instituta ovisi o radu informacijskog sustava Instituta.
- (4) Sigurnosna politika treba biti planirana i provedena na način da omogućava sigurno obavljanje posla, a da pritom ne ometa poslovne procese.
- (5) Institut može usvojiti i druge dokumente kojima se specificiraju pojedine odredbe ovog programa sigurnosti.

Članak 2.

- (1) Informacijski sustav (u daljnjem tekstu: IS) podrazumijeva usklađeno djelovanje svojih sastavnica:
 - Računalne i komunikacijske tehnologije;
 - Sustavskog i aplikativnog softvera;
 - Podataka/informacija;
 - Metoda i postupaka za obradu podataka;
 - Osoba koje održavaju IS, obrađuju podatke i koriste ih;
 - Poslovnih partnera i suradnika.
- (2) Informacijsku imovinu čini svaki resurs IS koji služi za prikupljanje, obradu, spremanje ili distribuciju podataka, na primjer:
 - Opipljiva (materijalna) imovina (zgrade, računala i komunikacijska oprema, infrastruktura);
 - Neopipljiva (nematerijalna) imovina (ugled, tehnologija, metodologija, zaštitni znak);
 - Podaci (dokumenti, ugovori, osobni podaci itd.);
 - Softver (sustavski i aplikativni programski paketi);
 - Ljudi koji održavaju i koriste IS.

(3) Sigurnost IS definira se kao skup mjera i postupaka, na tehničkoj i organizacijskoj razini, čijom se primjenom postiže i održava prihvatljiva razina rizika IS.

(4) Temeljna načela sigurnosti IS su:

- Povjerljivost – informacije su dostupne samo ovlaštenim ljudima i organizacijama;
- Cjelovitost – ažurnost i točnost podataka, sprječavanje neovlaštenog mijenjanja i uništavanja podataka;
- Dostupnost – podaci moraju biti na raspolaganju ovlaštenim korisnicima u trenutku kada su potrebni.

(5) Procjena rizika je postupak kojim se identificiraju prijetnje i ranjivosti koje mogu ugroziti rad IS.

- Za svaku prijetnju određuje se vjerojatnost ostvarenja i potencijalna šteta, kako bi se odredili prioriteti i odabrale mjere koje smanjuju rizik na prihvatljivu razinu.
- Procjena rizika provodi se periodički kako bi se ustanovile promjene u prijetnjama, ranjivostima i poslovnim prioritetima.
- Troškovi primjene sigurnosnih mjera moraju biti razmjerni osjetljivosti i vrijednosti informacija koje se takvim mjerama štite te prilagođeni materijalnim i ljudskim mogućnostima.

(6) Sigurnosni događaj je svaki događaj koji ukazuje na probleme koji ne ugrožavaju rad samog IS niti povjerljivost podataka (npr. kada korisnici zaborave zaporku).

(7) Sigurnosni incident je događaj koji ugrožava povjerljivost, integritet i dostupnost podataka, integritet sustavskog softvera i poslovnih aplikacija ili ukazuje na neovlašten pristup informacijskim resursima. Incidentom se smatraju i događaji koji onemogućavaju neprekidnost poslovanja, poput nestanka električne energije, poplave, požara itd.

Članak 3.

(1) Politika sigurnosti primjenjuje se na sve komponente IS.

(2) Pravila sigurnosne politike dužni su poštovati i provoditi svi zaposlenici, poslovni partneri i vanjski suradnici koji imaju pristup podacima i informacijskoj infrastrukturi u skladu s poslovnim potrebama.

Članak 4.

(1) Institut usvaja sljedeću strukturu dokumentacije koja se bavi informacijskom sigurnošću:

- Politika sigurnosti IS kao najviša razina dokumentacije definira temeljne odrednice za uspostavu sigurnog i učinkovitog IS;
- Pravilnici Instituta: Pravilnik o korištenju elektroničke pošte, Pravilnik o prihvatljivom korištenju računalne opreme i Pravilnik o korištenju lozinki detaljno opisuju mjere i pravila čijom se primjenom osigurava uspostava prihvatljive razine informacijske sigurnosti;
- Upute sadrže konkretne procedure i mjere koje treba slijediti u okviru pojedinih poslovnih procesa.

Članak 5.

(1) Pod informacijskom imovinom smatra se svaki materijalni ili nematerijalni resurs IS ili organizacijske strukture Instituta koji služi za prikupljanje, obradu, spremanje ili distribuciju informacija značajnih u poslovnom procesu.

(2) Podaci se smatraju naročito vrijednim oblikom informacijske imovine.

Članak 6.

(1) Korisnik je svaki zaposlenik, vanjski partner ili suradnik Instituta koji u skladu s poslovnim potrebama pristupa IS Instituta.

(2) Izvanrednu suglasnost za pristup IS i korištenje podataka unutarnjim i vanjskim korisnicima daje ravnatelj Instituta.

(3) Korisniku se smiju dodijeliti samo ovlasti potrebne za obavljanje njegovih redovitih poslova. Korisnik smije imati uvid samo u one podatke koji su neophodni za obavljanje njegovih poslovnih funkcija.

(4) Dužnosti korisnika su:

- Pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu s poslovnim procesima, etičkim normama i pravilima aktualne sigurnosne politike;
- Izbor kvalitetne zaporke i njezina povremena promjena;
- Prijava sigurnosnih događaja i incidenata;
- Korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. To znači da su dužni voditi računa o izradi sigurnosnih kopija, tj. ako nisu u mogućnosti moraju od voditelja organizacijskih jedinica zatražiti da uspostave automatsku sigurnosnu pohranu isključivo poslovnih podataka po unaprijed definiranim pravilima i strukturi;
- Korisniku je zabranjeno korištenje dodataka/programskih dodataka koje nije preporučila informatička podrška;
- Korisnici ne smiju namjerno sudjelovati u širenju zlonamjernih programa;
- Prilikom napuštanja prostorije korisnik mora adekvatno zbrinuti službene dokumente za koje je odgovoran i zaključati računalo. Ako osoba posljednja odlazi, dužna je ugasiti svjetlo u prostoriji, zatvoriti prozore i vrata, a ako je moguće ugasiti klime, grijalice i sl.;
- Korisniku kojemu je istekao radni odnos u Institutu u roku od 30 dana briše se elektronički identitet iz sustava AA@EduHR te se zatvara korisnički račun iz domene Instituta.

Članak 7.

(1) Ova se Politika odnosi na sigurnost IS, a sigurnim zonama smatraju se prostori od važnosti za njegovo funkcioniranje. Na dan donošenja dokumenta, u području informatičke, tj. informacijske sigurnosti, sigurne zone su komunikacijski čvorovi na poslovnim lokacijama Instituta (Trg Stjepana Radića 3, Zagreb; Hvarska 1e, Zagreb).

(2) Izbor i osiguranje navedenih prostora, smještaj opreme i radni uvjeti u sigurnim zonama moraju uzeti u obzir sigurnosne rizike i značaj resursa koji su u njima smješteni.

(3) Osjetljivi informacijski resursi moraju biti smješteni u posebno osiguranim dijelovima radne okoline, kako bi im se omogućili optimalni radni uvjeti (temperatura, vlažnost, zaštita od požara i sl.).

(4) Središnja računalna oprema mora biti smještena u sigurnoj zoni i mogu joj pristupati samo ovlašteni zaposlenici. Popis ovlaštenih zaposlenika izrađuje savjetnik za informacijsku sigurnost.

Članak 8.

(1) Računalni sustavi i mrežna oprema moraju biti konfigurirani tako da bilježe sustavsku i korisničku aktivnost, naročito događaje koji pružaju dokaze o pristupu povjerljivim ili osjetljivim podacima ili programima.

(2) Podsustav za kontrolu pristupa korisnika mora imati mogućnost konfiguracije koja će omogućiti zadovoljavajuću provjeru identiteta korisnika i kontrolu dodjele prava za rad.

(3) Administratori sustava dužni su slijediti sve stručne upute proizvođača komponenti koje čine IS.

(4) Popravke sustavskog programskog koda koje ispravljaju sigurnosne probleme moraju biti ocijenjene/provjerene i primijenjene u najkraćem mogućem roku.

Članak 9.

(1) Korištenje nezakonitog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Da bi se Institut zaštitio od moralne i materijalne štete koja time može nastati, savjetnik za informacijsku sigurnost vodi brigu o instaliranju softvera i njegovu licenciranju. Korisnik kojem je potrebna instalacija korisničkog programa, mora se obratiti voditelju organizacijske jedinice i zatražiti, uz obrazloženje, nabavu i instalaciju.

(2) U slučaju povrede autorskih prava i intelektualnog vlasništva korisnici odgovaraju za nastalu materijalnu i nematerijalnu štetu, a za unutarnje korisnike pokreću se i ostali postupci sukladno propisima iz radnog odnosa.

Članak 10.

(1) Pri projektiranju novih ili unaprjeđenju postojećih IS, savjetnik za informacijsku sigurnost definirat će sigurnosne zahtjeve i mjere neophodne za siguran rad sustava.

(2) Isti zahtjevi vrijede i kod razmatranja gotovih programskih paketa.

(3) Pristup izvornom programskom kodu mora biti ograničen i kontroliran. Izvršni se kod može primijeniti u produkcijskom okruženju samo nakon postupka testiranja, prihvatanja i odobrenja.

(4) Probni podaci koji se koriste u svrhu testiranja programa moraju biti zaštićeni, a pristup takvim podacima kontroliran. Korištenje zaštićenih podataka, primjerice osobnih podataka, u svrhu testiranja nije dopušteno, osim ako su depersonalizirani.

(5) Programski sustavi moraju imati mogućnost bilježenja početka i izvora pojedinih transakcija te podatke o svakom pristupu i akciji nad osjetljivim podacima.

(6) Svaka promjena na sustavu mora biti detaljno planirana, izvođenje promjene odobreno, a rezultati promjene dokumentirani.

(7) Svaki novi resurs IS mora prije početka produkcijskog korištenja, u suradnji s djelatnikom zaduženim za upravljanje licencama proći kroz postupak provjere i odobravanja, kako bi se mogla jamčiti njegova ispravnost i mogućnost obavljanja očekivanih funkcija.

Članak 11.

- (1) Pravo pristupa informacijama, informacijskim resursima i procesima IS, može biti dodijeljeno samo na temelju odobrenja voditelja organizacijske jedinice uz suglasnost savjetnika za informacijsku sigurnost.
- (2) Svakom korisniku pojedine aplikacije ili informacijskog servisa mora biti dodijeljeno jedinstveno korisničko ime za takvu aplikaciju ili servis. Svako korisničko ime mora imati svoju lozinku.
- (3) Davatelji usluga nadležni su za kontrolu, autorizaciju i nadzor pristupa korisnika.
- (4) Korisnik je dužan odabrati svoju lozinku na način kako je to opisano u Pravilniku o korištenju lozinki.
- (5) Korisnik je obavezan čuvati svoju lozinku i ne odavati je drugim osobama.

Članak 12.

- (1) Potrebno je redovito izrađivati zaštitne kopije produkcijskih podataka. Odgovornost i upute za izradu zaštitnih kopija moraju biti određeni posebnim postupcima.
- (2) Odluka o načinu spremanja zaštitnih kopija, kao i njihovom broju formira se na temelju važnosti podataka, u skladu s mogućnostima. Ovu odluku donosi ravnatelj na temelju prijedloga savjetnika za informacijsku sigurnost. Prema potrebi, zaštitne kopije mogu biti spremljene izvan glavne lokacije Instituta.
- (3) Davatelj informatičkih usluga dužan je osigurati odgovarajuće resurse za obnovu podataka sa zaštitnih kopija.
- (4) Postupak obnove podataka sa zaštitnih kopija mora se izvoditi sukladno zahtjevu određenom na temelju procjene rizika.

Članak 13.

- (1) Obrada, pohrana i korištenje podataka na osobnim računalima moraju biti provedeni tako da se spriječe sigurnosni rizici.
- (2) Korisnici osobnih računala moraju slijediti upute za zaštitu od računalnih virusa ili drugih destruktivnih programa. U slučaju pojave računalnog virusa ili drugih destruktivnih programa, korisnici moraju odmah obavijestiti voditelja organizacijske jedinice te postupiti prema uputama.

Članak 14.

- (1) Računalni resursi smiju se koristiti isključivo za svrhe poslovnog procesa Instituta.
- (2) Korisnici su odgovorni za profesionalno, etičko i zakonito korištenje računalnih resursa koji su im dani na raspolaganje.
- (3) Korištenje programskih paketa mora biti u skladu sa zakonom i uvjetima licencije.
- (4) S obzirom da kapaciteti mrežnih i računalnih resursa Instituta imaju svoja ograničenja, od svih korisnika se očekuje korištenje računalnih resursa na način koji neće onemogućiti ili smanjiti učinkovitost rada drugih korisnika.

Članak 15.

- (1) Elektroničkom poštom korisnici se služe isključivo radi obavljanja posla. Pri sastavljanju pisama dužni su čuvati ugled Instituta. Korisnici ne smiju slati elektroničkom poštom ili bilo

kojom drugom formom elektroničke komunikacije informacije koje bi za druge osobe mogle biti uvredljive ili klevetničke. Elektroničkom se poštom ne smiju slati neistinite informacije u namjeri da nanesu štetu trećim osobama.

(2) Pošiljatelji su odgovorni za istinitost i pouzdanost informacija koje se prenose elektroničkom poštom. Elektronička se pošta mora koristiti uvažavajući ista pravila ponašanja kao i u bilo kojem drugom obliku pisane komunikacije.

(3) Podaci koji su klasificirani nekom od oznaka tajnosti mogu biti poslani elektroničkom poštom tek uz dopuštenje osobe odgovorne za te podatke, uz suglasnost ravnatelja i uz primjenu enkripcije.

(4) Korisnici moraju biti svjesni da korištenje elektroničkih poruka ne podrazumijeva privatnost i sigurnost samih poruka.

(5) Savjetnik za informacijsku sigurnost zadužen je za provedbu tehničkih mjera kojima se smanjuje rizik korištenja elektroničke pošte, što uključuje zaštitu od virusa i neželjenih poruka (spama).

Članak 16.

(1) Internet se smatra značajnom komponentom IS Instituta koja se prije svega može koristiti za poslovnu namjenu, informiranje i edukaciju.

(2) Savjetnik za informacijsku sigurnost odgovoran je za provedbu odgovarajućih mjera kojima se onemogućuje neovlašten pristup unutarnjoj mreži ili podacima Instituta putem Interneta.

(3) Korisnici su dužni izbjegavati aktivnosti koje bi mogle ugroziti sigurnost njihovih računala i IS Instituta.

(4) Savjetnik za informacijsku sigurnost dužan je osigurati provedbu mjera na tehničkoj i organizacijskoj razini, uključujući edukaciju, kojima se smanjuju rizici korištenja Interneta.

Članak 17.

(1) Potrebno je definirati i provesti mjere zaštite od virusa i drugih destruktivnih programa na svim osobnim računalima i poslužiteljima.

(2) Mjere zaštite od virusa podrazumijevaju korištenje programa za zaštitu od virusa, ali i uzdržavanje korisnika od radnji koje ugrožavaju sigurnost IS.

(3) Korisnici moraju biti upoznati s postupkom zaštite od virusa, uključujući praćenje redovitih informacija o sigurnosnim mjerama.

(4) Programi koji služe za zaštitu od virusa moraju biti redovito ažurirani i dograđivani.

(5) Korisnici ne smiju isključivati ili onemogućavati programe za zaštitu od virusa.

Članak 18.

(1) Svaki događaj koji ukazuje na pojavu sigurnosnog incidenta mora biti prijavljen voditelju organizacijske jedinice u najkraćem mogućem roku.

(2) Ako je utjecaj sigurnosnog incidenta takav da je raspoloživost sustava znatno smanjena, primjenjuju se odredbe politike sigurnosti o osiguranju neprekidnosti radnog procesa.

(3) Potrebno je definirati procedure odgovaranja na sigurnosne incidente i odgovornosti svih sudionika u njihovoj provedbi. Postupak odgovora na sigurnosne incidente mora omogućiti brz i učinkovit odgovor na sve potencijalne vrste incidenata.

- (4) Postupak odgovora na sigurnosne incidente mora uključivati i postupak obnove sustava nakon incidenata.
- (5) Zaposlenici Instituta dužni su obavijestiti voditelja organizacijske jedinice o svim slabim točkama ili ranjivostima produkcijskih sustava.
- (6) Bez prethodne dozvole ravnatelja, zaposlenici ne smiju javno objavljivati podatke o pojavi sigurnosnih incidenata, problema ili ranjivosti sustava i računalne mreže Instituta.
- (7) Iznimku predstavljaju slučajevi koji su regulirani zakonskim i podzakonskim propisima.

Članak 19.

- (1) Dijelovi IS koji obavljaju kritične funkcije moraju imati plan kontinuiteta poslovanja u slučaju izvanrednih okolnosti.
- (2) Pod izvanrednim okolnostima smatraju se događaji koji mogu uzrokovati gubitak povjerljivosti i integriteta podataka ili sustava te prekid ili smanjenje raspoloživosti IS.
- (3) Prije donošenja plana potrebno je provesti postupak procjene rizika. Plan kontinuiteta poslovanja mora definirati mjere koje će biti sukladne predviđenim rizicima.
- (4) Plan djelovanja u slučaju izvanrednih okolnosti mora uključivati postupak odgovaranja na incidente, rezervni plan obavljanja funkcija i obnavljanje redovitih funkcija.
- (5) Provedba plana kontinuiteta poslovanja podrazumijeva i provedbu preventivnih mjera kojima se smanjuje rizik pojave incidenata.

Članak 20.

- (1) Institut zadržava pravo nadzora i bilježenja svih aktivnosti na računalnim resursima te provođenja redovitih provjera pridržavanja sigurnosne politike. Savjetnik za informacijsku sigurnost dužan je osigurati provjeru stanja sigurnosti pojedinih komponenti IS, sustavskih zapisa o radu IS, evidenciju o radu korisnika i druge sustavske podatke radi otkrivanja sigurnosnih incidenata i nepridržavanja politike sigurnosti.
- (2) Bilježenje aktivnosti na računalnim resursima može obuhvatiti i bilježenje aktivnosti te podataka koji nisu vezani za poslovne procese Instituta.
- (3) Institut zadržava pravo provjere svake datoteke ili poruke elektroničke pošte koja je izrađena, spremljena ili prosljeđena računalnim resursima Instituta, što uključuje i pravo provjere datoteka ili poruka s privatnim sadržajem koje se nalaze u mapama ili direktorijima korisnika.
- (4) Provjera se može obaviti radi:
 - istrage o sigurnosnim incidentima;
 - provjere jesu li IS i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike;
 - osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa.

Nadzor smiju obavljati samo osobe koje je ravnatelj Instituta za to ovlastio. Prilikom provedbe provjere, ovlaštene osobe dužne su poštovati privatnost korisnika i podataka. Ako je korisnik prekršio pravila sigurnosne politike, povjerljivost informacija ne mora se osigurati i može se pregledati sav sadržaj na računalu, uključujući i onaj koji korisnik smatra privatnim.

Članak 21.

(1) Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama Instituta i priključena je u mrežu CARNet, na sav instalirani softver te na sve mrežne servise. Pravila su dužni poštivati i provoditi svi zaposlenici, studenti i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Članak 22.

(1) Korisnici su dužni pomoći osobama zaduženima za nadzor IS tako da im pruže sve potrebne informacije te im omoguće pristup prostorijama i opremi radi provođenja nadzora. Isto vrijedi i za administratore računala i pojedinih servisa, koji su dužni savjetnicima za informacijsku sigurnost pomagati pri istrazi.

Pristup uključuje:

- Pristup svojoj računalnoj opremi na razini korisnika ili sustava;
- Pristup svakoj informaciji, u elektroničkom ili tiskanom obliku, koja je proizvedena ili pohranjena na opremi Instituta ili se prenosi putem te opreme;
- Pristup radnom prostoru;
- Pravo na interaktivno nadgledanje i bilježenje prometa na mreži Instituta.

Članak 23.

Ova Politika stupa na snagu osam (8) dana nakon dana objave na mrežnim stranicama Instituta.

KLASA: 007-01/26-02/06

URBROJ: 03/01-26-1

Zagreb, 22. rujna 2026.

Predsjednik Upravnog vijeća

dr. sc. Mladen Vedriš

Utvrđuje se da je ova *Politika sigurnosti informacijskog sustava* objavljena na mrežnoj stranici Instituta dana 25. 09. 2026. godine te da je na snagu stupila dana 05. 10. 2026. godine.

Ravnateljica

dr. sc. Marina Perić Kaselj