



Na temelju članka 29. t. 12. Statuta Agencije za plaćanja u poljoprivredi, ribarstvu i ruralnom razvoju (dalje u tekstu: Agencija), ravnatelj Agencije za plaćanja donosi

POLITIKU INFORMACIJSKE SIGURNOSTI

I. OPĆE ODREDBE

Članak 1.

- (1) Informacijska sigurnost je zaštita informacija od širokog opsega prijetnji s ciljem osiguranja poslovnog kontinuiteta, minimiziranja poslovnog rizika i maksimiziranja povrata investicija i poslovnih prilika.
- (2) Učinkovito upravljanje informacijskom sigurnošću nužno je za izvršavanje svih poslovnih procesa u Agenciji za plaćanja.
- (3) Nizom kontrolnih mehanizama te uspostavljenom strukturom odgovornosti, proceduralnih, tehničkih i organizacijskih mjera, Agencija za plaćanja želi osigurati da je informacijska sigurnost sastavni dio svih njenih poslovnih procesa, djelovanja i rukovođenja.
- (4) Sustav upravljanja informacijskom sigurnošću upravlja se prema standardu ISO/IEC 27001:2022.
- (5) Svi zaposlenici, treće pravne ili fizičke osobe moraju se ponašati u skladu s odredbama ove politike, svim slijednim pravilnicima i procedurama, tehničkim i organizacijskim sigurnosnim mjerama, te svim poslovnim, pravnim i regulatornim zahtjevima informacijske sigurnosti.
- (6) Glavni prateći dokument ove Politike je Pravilnik o upravljanju informacijskom sigurnošću koji na detaljan način definira i objašnjava uspostavu i provedbu kontrola za postizanje zadovoljavajućeg nivoa informacijske sigurnosti.

- (7) Zaposlenici i treće osobe na bilo koji način uključene u poslovne procese Agencije za plaćanja dužni su redovito se upoznavati sa odredbama informacijske sigurnosti. Na taj način preuzimaju i odgovornost za informacijsku sigurnost, a u slučaju povrede istih odgovaraju sukladno ugovornim obvezama i internim aktima Agencije za plaćanja.

Članak 2.

Područje valjanosti

- (1) Politika informacijske sigurnosti se odnosi na sve poslovne procese Agencije za plaćanja, cjelokupnu informacijsku strukturu, uključujući podatke, softver, hardver, medije za podatke, sredstva, komunikacijsku opremu; osobe odgovorne za administraciju informacijskog sustava; sve zaposlenike i korisnike sustava, odnosno osobe koje imaju pravo pristupa; vanjske suradnike (npr. ovlaštene djelatnike zadužene za održavanje sustava).

Članak 3.

Ciljevi informacijske sigurnosti

- (1) Ciljevi informacijske sigurnosti su sljedeći:
- a) Primijeniti odgovarajući skup kontrola, uključujući pravilnike, procese, procedure, organizacijske strukture, softverske i hardverske funkcije kako bi se postigla željena razina informacijske sigurnosti i time osiguralo ispunjenje poslovnih ciljeva organizacije, uz uvažavanje ostalih poslovnih upravljačkih procesa.
 - b) Postaviti učinkovitu strukturu odgovornosti za primjenu odredbi politike informacijske sigurnosti.
 - c) Definirati metode i postupke za primjenu sigurnosti i zaštite informacijskih sustava Agencije za plaćanja.
 - d) Osigurati da su rizici informacijske sigurnosti na poslovno prihvatljivoj razini
 - e) Minimizirati broj incidenata informacijske sigurnosti.

Članak 4.

- (1) Primjena politike informacijske sigurnosti se redovito osigurava putem:
- a) Uspostave i održavanja učinkovitog sustava ovlasti i odgovornosti za informacijsku sigurnost.
 - b) Primjenjivanja potrebnih sigurnosnih kontrola na temelju procjene i upravljanja rizicima informacijske sigurnosti, te njihove opravdanosti, funkcionalnosti, isplativosti i učinkovitosti.
 - c) Implementacijom, održavanjem, nadzorom i poboljšanjem svih potrebnih organizacijskih, proceduralnih i tehničkih sigurnosnih mjera.

- (2) Kontrola primjene politike informacijske sigurnosti mora se provoditi redovito kroz aktivnosti interne prosudbe upravljanja informacijskom sigurnošću te provjeru učinkovitosti implementiranih sigurnosnih kontrola.
- (3) Revidiranje politike informacijske sigurnosti provodi se jednom godišnje dok se ažuriranje mora provesti u slučaju većih promjena u poslovanju Agencije za plaćanja kako bi se osigurala njena prikladnost i učinkovitost.
- (4) Ažuriranje politike informacijske sigurnosti uključuje i procjenu prilika za poboljšanje politike informacijske sigurnosti kao odgovor na organizacijske i tehnološke promjene, te poslovne i zakonske prilike.

II. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 5.

- (1) Stupanjem na snagu ove Politike prestaje važiti Politika informacijske sigurnosti, KLASA: 600-01/23-01-01/0001, URBROJ: 343-0702/11-23-001 od 2. veljače 2023. godine.
- (2) Politika stupa na snagu danom donošenja.



KLASA: 600-01/25-01-01/0001
URBROJ: 343-0100/09-25-001

Zagreb, 4. travnja 2025. godine