

Na temelju članka 7. Zakona o Poreznoj upravi („Narodne novine“, broj 148/13 i 141/14), a sukladno Pravilniku o primjerenom korištenju informacijskog sustava, KLASA: 011-01/11-01/402, pomoćnik ministra, ravnatelj Porezne uprave donosi

## **POLITIKU SIGURNOSTI INFORMACIJSKOG SUSTAVA MINISTARSTVA FINACIJA - POREZNE UPRAVE**

### **I. UVODNE ODREDBE**

#### **Članak 1.**

Politika sigurnost informacijskog sustava (u daljnjem tekstu: Politika sigurnosti) Ministarstva financija - Porezne uprave (u daljnjem tekstu: Porezna uprava) predstavlja najvišu razinu dokumentacije vezane za sigurnost Informacijskog sustava Porezne uprave, opća pravila kojima se uređuju pitanja povjerljivosti, cjelovitosti i raspoloživosti podataka primjenom propisanih mjera i standarda informacijske sigurnosti kao i organizacijska podrška za poslove planiranja, provedbe, provjere i dorade mjera i standarda.

Informacijski sustav je računalni, komunikacijski ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose tako da budu dostupni i uporabljivi za korisnike informacijskog sustava, a koji obuhvaća tehničku infrastrukturu, organizaciju, osobe i postupke kojima se podaci obrađuju, pohranjuju ili prenose.

#### **Članak 2.**

Politikom sigurnosti se definiraju načela sigurnosti Informacijskog sustava Porezne uprave.

Sukladno Politici sigurnosti donose se i ostali akti koji reguliraju pitanja vezana uz pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima pohranjenim unutar Informacijskog sustava Porezne uprave.

Porezna uprava može usvojiti i druge standarde i mjere, upute i procedure kojima će pobliže urediti pojedina pitanja politike sigurnosti.

#### **Članak 3.**

Politikom sigurnosti se definiraju načela i osnovni principi aspekta sigurnosti pružanja usluga Informacijskog sustava Porezne uprave te odgovornosti koje se odnose na upravljanje procesima Informacijskog sustava Porezne uprave.

Osnovni principi koje pri tome treba poštivati su:

- Integralnost: osigurati integritet i cjelovitost informacijskog sustava,
- Raspoloživost: osigurati nesmetano i neprekidno odvijanje poslovnih procesa,
- Povjerljivost: osigurati da informacije budu dostupne samo ovlaštenim subjektima,
- Pouzdanost: osigurati dosljedno, očekivano ponašanje i rezultat,
- Odgovornost: dužnosti i odgovornosti moraju biti jasno opisane i prihvaćene,

- Pravovremenost: pravovremeno reagirati na moguće ugrožavanje pružanja informacijske usluge,
- Provjerljivost: redovna provjera kvalitete informacijske usluge i procjena rizika za informacije i informacijski sustav.

## II. PRIMJENA

### Članak 4.

Službenici i namještenici Porezne uprave zaposleni na neodređeno ili određeno vrijeme, ostale osobe koje su na bilo koji način uključeni u poslovne procese Porezne uprave temeljem ugovorne obveze ili drugih obveza, poslovni suradnici koji na bilo koji način dolaze u doticaj s resursima Informacijskog sustava Porezne uprave (u daljnjem tekstu: korisnici) dužni su se pridržavati odredbi Politike sigurnosti te ostalih pravila donesenih temeljem Politike sigurnosti, u cilju osiguranja pravilnog rada Informacijskog sustava, u svrhu očuvanja neprekidnog poslovanja.

### Članak 5.

Odredbe Politike sigurnosti i svih akata donesenih na temelju Politike sigurnosti, kao i temeljem zakona kojima se uređuje područje informacijske sigurnosti u Republici Hrvatskoj, primjenjuju se na sve resurse informacijskog sustava i vezane organizacijske strukture Porezne uprave i ostale resurse informacijskih sustava koji ugovorno podržavaju poslovanje Porezne uprave.

## III. SVRHA

### Članak 6.

Provedbeni dokumenti: standardi, mjere, upute i procedure doneseni na temelju Politike sigurnosti imaju za svrhu osigurati:

- odgovarajuću fizičku zaštitu, kvalitetu upravljanja te pravilno zbrinjavanje opreme za obradu podataka i okoline u kojoj je takva oprema smještena,
- održavanje cjelovitosti aplikacija i podataka,
- ispravno i pravodobno pružanje usluga informacijskog sustava,
- stalni nadzor nad pružanjem usluga informacijskog sustava,
- ovlašteno i odgovorno korištenje informacijsko - komunikacijskog sustava,
- jasno formilirane zahtjeve za informacijskom uslugom,
- ovlašteno postupanje s informacijama,
- uvid u klasificirane podatke ovlaštenim osobama,
- ispunjavanje svih drugih zakonskih ili ugovornih obveza o zaštiti podataka.

#### IV. DEFINICIJE

##### Članak 7.

Resursi informacijskog sustava su hardverska, softverska i informacijska imovina te korisnici informacijskog sustava.

Hardverska imovina su računala i računalna oprema, komunikacijska oprema, sustavi za pohranu podataka te ostala tehnička oprema koja podržava rad informacijskog sustava.

Softverska imovina su operativni sustavi, programi za nadzor informacijskih sustava, sigurnosni programi, korisnički programi, programi za upravljanje bazama podataka, alati za razvoj programa, uslužni programi i ostali programi koji se nalaze na informacijskim sustavima.

Informacijska imovina su podaci u bazama podataka, datoteke s podacima, programski kod u tekstualnom obliku, dokumentacija o informacijskim sustavima i programima, priručnici, planovi i usluge informacijskog sustava te cjelokupni edukacijski materijal koji služi podršci poslovanju.

Korisnici informacijskog sustava su službenici i namještenici Porezne uprave, djelatnici partnerskih tvrtki koji osiguravaju ispravan i neprekinuti rad informacijskog sustava, ostali korisnici kojima je dodijeljeno pravo pristupa odnosno uporabe informacijskog sustava.

#### V. OVLAŠTI I ODGOVORNOSTI ZA PROVEDBU POLITIKE SIGURNOSTI

##### Članak 8.

Ravnatelj Porezne uprave donosi:

1. Pravila o provedbi politike sigurnosti Informacijskog sustava Ministarstva financija Porezne uprave,
2. Pravila o sigurnosnim mjerama pristupa Informacijskom sustavu Ministarstva financija- Porezne uprave za vanjske suradnike,
3. Uputu za korištenje Informacijskog sustava Ministarstva financija- Porezne uprave,
4. Uputu za korištenje sustava elektroničke pošte i interneta Ministarstva financija Porezne uprave,
5. Uputu za evidenciju pristupa informatičkoj opremi
6. Uputu za upravljanje korisničkim računima.

Ravnatelj Porezne uprave donosi i druge standarde, mjere te procedure vezano za sigurnost informacijskog sustava.

##### Članak 9.

Služba nadležna za informacijsko – komunikacijski sustav sudjeluje u izradi i provodi mjere provedbe politike sigurnosti te obavlja kontinuirani nadzor rada informacijskog sustava Porezne uprave.

Savjetnik za informacijsku sigurnost sudjeluje u izradi i ovlašten je za provedbu i nadzor provedbe Politike sigurnosti, izvještava ravnatelja Porezne uprave o stanju sigurnosti Informacijskog sustava, odstupanjima od Politike sigurnosti kao i o svakom pojedinačnom slučaju kršenja ili postupanja protivno Politici sigurnosti.

Savjetnik za informacijsku sigurnost provodi nadzor efikasnosti primjene i provedbe politike sigurnosti i ostalih standarda i mjera, uputa i procedura donesenih na temelju Politike sigurnosti i ostalih propisa Republike Hrvatske u području informacijske sigurnosti.

Svi službenici i namještenici Porezne uprave koji koriste Informacijski sustav Porezne uprave odgovorni su za provođenje mjera Politike sigurnosti sukladno svojim ovlastima.

Izjavom o prihvaćanju Politike sigurnosti Informacijskog sustava Ministarstva financija - Porezne uprave i Pravila o provedbi politike sigurnosti Informacijskog sustava Ministarstva financija - Porezne uprave korisnici su odgovorni za provođenje mjera Politike sigurnosti.

#### Članak 10.

Povjerenstvo za informacijsku sigurnost imenuje Ravnatelj Porezne uprave na prijedlog savjetnika za informacijsku sigurnost Porezne uprave.

Povjerenstvo za informacijsku sigurnost predlaže izmjene Politike sigurnosti.

Povjerenstvo za informacijsku sigurnost sastoji se od 8 (osam) članova. Predsjednik i većina članova povjerenstva su službenici Porezne uprave.

Za člana povjerenstva može biti imenovan vanjski suradnik sukladno ugovornim obvezama.

Sastanci Povjerenstva za informacijsku sigurnost održavaju se u pravilu dvaput godišnje, a prema potrebi i češće.

### VI. IZMJENE POLITIKE SIGURNOSTI

#### Članak 11.

Povjerenstvo za informacijsku sigurnost po potrebi usklađuje i predlaže ravnatelju Porezne uprave promjenu Politike sigurnosti i svih ostalih standarda i mjera, uputa i procedura donesenih na temelju Politike sigurnosti.

### VII. OBAVJEŠTAVANJE O KRŠENJU ODREDBA POLITIKE SIGURNOSTI

#### Članak 12.

Osobe iz članka 4. ove Politike sigurnosti obvezne su o narušavanju pravila Politike sigurnosti i svih ostalih standarda i mjera, uputa i procedura donesenih na temelju Politike sigurnosti obavijestiti nadređenu osobu koja o tome izvješćuje službenike ovlaštene za provedbu i nadzor provedbe Politika sigurnosti iz članka 9 ove Politike sigurnosti

Dužnost obavještavanja iz prethodnog stavka odnosi se i na bilo koji slučaj neovlaštenog otkrivanja klasificiranih podataka Porezne uprave trećim osobama.

### Članak 13.

Nepridržavanje odredbi politike sigurnosti i svih ostalih standarda i mjera, uputa i procedura donesenih na temelju Politike sigurnosti predstavlja tešku povredu službene dužnosti.

### Članak 14.

Svi službenici i namještenici obvezni su potpisati izjavu kojom prihvaćanju Politike sigurnosti te ostalih pravila donesenih na temelju politike sigurnosti, uputa za korištenje informacijskog sustava i drugih standarda, mjera i procedura vezanih za sigurnost informacijskog sustava.

### Članak 15.

Ova Politika sigurnosti stupa na snagu danom donošenja.

KLASA: 043-01/16-01/192  
URBROJ: 513-07-21-14-16-3

Zagreb, 16. svibnja 2016. godine

**POMOĆNIK MINISTRA  
RAVNATELJ**  
  
Zdravko Zrinušić