

Na podlagi prvega odstavka 80. člena Uredbe o upravnem poslovanju (Uradni list RS, št. 20/2005, 106/2005, 30/2006, 86/2006, 32/2007, 63/2007, 115/2007, 31/2008 in 35/2009)
generalna direktorica Statističnega urada Republike Slovenije izdaja naslednjo

Politiko varovanja informacij Statističnega urada Republike Slovenije

VSEBINA

1	NAMEN IN CILJI POLITIKE VAROVANJA INFORMACIJ.....	3
2	OBSEG IN TEMELJNA NAČELA VAROVANJA INFORMACIJ	3
2.1	Obseg	3
2.2	Načela	3
2.3.	Dokumenti informacijske varnosti.....	5
2.4.	Kontrolno okolje in upravljanje s tveganji	5
3	INFORMACIJSKI VIRI.....	6
3.1	Opis informacijskih virov	6
3.2	Skrbnik.....	6
3.3	Klasifikacija informacij	6
4	ORGANIZIRANOST VAROVANJA INFORMACIJ	7
4.1	Pristojnosti in odgovornosti	7
5	KONČNE DOLOČBE.....	10
	PRILOGA 1: Izjava o seznanitvi s politiko varovanja informacij in podrejenimi področnimi pravilniki.....	11

1 NAMEN IN CILJI POLITIKE VAROVANJA INFORMACIJ

Namen Politike varovanja informacij (v nadaljevanju tudi: krovna varnostna politika) je vzpostavitev celostnega sistema upravljanja varovanja informacij (SUVI) in podatkov v Statističnem uradu Republike Slovenije (v nadaljevanju: Urad), s ciljem zagotavljanja delovanja Urada v skladu z zakonskimi in poslovnimi zahtevami.

Varovanje informacij in podatkov predstavlja nabor tehničnih in organizacijskih ukrepov, katerih cilj je varovanje in zagotavljanje celovitosti, razpoložljivosti, uporabnosti, dostopnosti in zaupnosti informacij in podatkov, ki jih obdeluje ter pripravlja Urad ter zagotavljanje neprekinjenosti delovanja Urada. Upravljanje informacijske varnosti mora biti usklajeno z drugimi organizacijskimi procesi. Ukrepi varovanja informacij se izvajajo za zaščito pred širokim naborom groženj oz. za zmanjševanje škode, ki bi izhajala iz uresničitve teh groženj. Za uspešno doseganje tega cilja je potrebno vzpostaviti in vzdrževati ustrezen nivo varnostne zavesti in kulture varovanja informacij pri vseh zaposlenih Urada – ti morajo poznati in ravnati v skladu z ustrežno zakonodajo in vsemi notranjimi pravili s področja varovanja informacij.

Eden ključnih ukrepov za izvajanje primerne informacijske varnosti na Uradu je zagotavljanje revizijske sledi obdelave podatkov.

Ukrepi varovanja informacij se prilagajajo organizacijskim, poslovnim ter strateškim ciljem Urada in veljavni zakonodaji. Sistem upravljanja varovanja informacij predstavlja temelj za zmanjševanje informacijskih tveganj, s čemer se zagotovi uspešno izvajanje nalog in poslovnih aktivnosti Urada.

2 OBSEG IN TEMELJNA NAČELA VAROVANJA INFORMACIJ

2.1 Obseg

Krovna varnostna politika predstavlja osnovni dokument upravljanja varovanja informacij in podatkov v Uradu. Politika vsebuje splošne smernice in načela varovanja informacij in podatkov Urada, nanaša pa se na vse informacijske vire Urada. Skupaj s pravilniki, postopki in drugimi dokumenti, naštetimi v Prilogi, predstavlja formalni okvir sistema upravljanja varovanja informacij na Uradu.

Namenjena je zaposlenim v Uradu, smiselno pa tudi pogodbenim sodelavcem, zunanjim izvajalcem ter vsem drugim osebam, ki pridobijo dostop do informacijskih virov Urada. Vsi našteti so odgovorni za spoštovanje te politike ter vseh drugih pravilnikov informacijske varnosti, ter za spoštovanje vseh organizacijskih in tehničnih ukrepov, ki se navezujejo na varovanje informacij na Uradu.

2.2 Načela

Sistem upravljanja varovanja informacij v Uradu predstavljajo pričujoča krovna varnostna politika ter področne politike, pravilniki in postopki, ki obravnavajo specifične organizacijske in tehnološke vidike informacijske varnosti.

Celostni sistem upravljanja varovanja informacij v Uradu je zasnovan na priporočilih standarda informacijske varnosti ISO 27001:2005 in je usklajen z načeli, vsebovanimi v krovni evropski uredbi, ki ureja evropsko statistiko, z zahtevami zakona, ki ureja državno statistiko, zakona, ki ureja varstvo osebnih podatkov, zakona, ki ureja tajne podatke in priporočili informacijske varnostne politike Ministrstva za javno upravo.

Vsak zaposleni je odgovoren za aktivno sodelovanje pri zagotavljanju varovanja informacij, predvsem pa za skrbno javljanje opaženih pomanjkljivosti pri aktivnostih varovanja informacij ter kršitev te politike ali drugih politik, pravilnikov in postopkov varovanja informacij nadrejenim oz. Odboru za sistem upravljanja varovanja informacij (v nadaljevanju: OSUVI).

Vsak zaposleni mora biti pred začetkom opravljanja dela v Uradu seznanjen s politiko varovanja informacij ter z dolžnostmi in odgovornostmi za varovanje informacij. Prav tako mora biti vsak zaposleni v Uradu formalno zavezan k spoštovanju te politike ter drugih pravilnikov za varovanje informacij, ki jih Urad sprejme. Obrazec izjave, ki jo mora podpisati vsaka oseba, ki z Uradom sklepa delovno ali drugačno poslovno razmerje, se nahaja v Prilogi 1 te krovne varnostne politike.

Sistem upravljanja varovanja informacij temelji na kontinuiranem razvoju, izboljševanju, izobraževanju vseh zaposlenih ter na poviševanju splošne zavesti o pomembnosti varovanja informacij v Uradu. V ta namen se za vse zaposlene izvajajo periodična izobraževanja s področja varovanja informacij, ki so prilagojena glede na tveganja, ki izhajajo iz posameznih vlog zaposlenih na Uradu.

Dejanja, ki so v nasprotju z načeli varovanja informacijskih virov Urada, predstavljajo kršitev delovnih obveznosti. Kršitve te politike se smatrajo kot kršitve pogodbe o zaposlitvi oziroma druge pogodbe, ki ureja pravni odnos, na podlagi katerega oseba pridobi dostop do informacijskih virov Urada. Postopek se izvaja v skladu z veljavnimi predpisi. Pri presojanju kršitev in izbiri sankcije se upošteva način kršenja politike, teža kršitve, število kršitev in druge okoliščine, relevantne za odločitev.

Urad lahko v primeru hujših kršitev proti kršiteljem uporabi vsa pravna sredstva, ki so na voljo, vključno z vložitvijo kazenske ovadbe v primeru suma storitve kaznivega dejanja ali vložitve odškodninskega zahtevka.

Varovanje informacij Urada se izvaja v skladu z veljavno zakonodajo Republike Slovenije, ki se nanaša na delovno področje Urada.

Krovna varnostna politika je predmet periodičnega pregleda. Krovna varnostna politika se dopolnjuje in razvija skladno z dejanskimi potrebami Urada. Viri informacij za dopolnitev in nadgradnjo krovne varnostne politike so lahko med drugim:

- 🔑 povratne informacije,
- 🔑 varnostni incidenti,
- 🔑 rezultati neodvisnih pregledov,
- 🔑 rezultati notranjih pregledov,
- 🔑 status preprečevalnih in popravljalnih kontrolnih aktivnosti,
- 🔑 učinkovitost procesov ter upoštevanje načel informacijske varnosti v rednem delovanju,
- 🔑 spremembe v organizacijskem okolju, vključno s spremembami v pravnih, poslovnih, tehničnih in drugih pogojih delovanja,
- 🔑 trendi groženj in ranljivosti,
- 🔑 priporočila pristojnih nadzornih organov.

O spremembah krovne varnostne politike in posameznih področnih pravilnikov se vsakokrat seznani vse zaposlene v Uradu preko službene e-pošte in z objavo na intranetu.

2.3. Dokumenti informacijske varnosti

Celostni sistem upravljanja varovanja informacij v Uradu je zastavljen v obliki varnostnih pravilnikov, postopkov in drugih dokumentov. Krovna varnostna politika predstavlja osnovni dokument za organizacijo varovanja informacij v Uradu. Na podlagi krovne varnostne politike se sprejmejo podrejeni dokumenti, ki urejajo posamezne postopke in ukrepe upravljanja varovanja informacij. To so:

- 🔑 **Pravilniki**, ki vsebujejo pravila o uporabi in upravljanju z informacijskimi viri, način njihove zaščite, varnostni mehanizmi in nivo njihovega varovanja, ustrezna uporaba posameznih virov ter odgovornosti in vloge posameznih zaposlenih pri upravljanju teh virov;
- 🔑 **Operativni postopki**, ki vsebujejo natančna pravila o ravnanju z informacijskimi viri;
- 🔑 **Navodila**, ki natančneje opredeljujejo ravnanje zaposlenih;
- 🔑 **Priročniki**, ki so skupki pravil za določeno skupino informacijskih virov ali za določeno skupino zaposlenih.

2.4. Kontrolno okolje in upravljanje s tveganji

Ukrepi varovanja informacijskih virov Urada so zasnovani na okviru upravljanja tveganj. Varovanje informacijskih virov se izvaja glede na izpostavljenost tveganjem. Informacijski viri so izpostavljeni različnim grožnjam, iz te izpostavljenosti pa izhajajo različna tveganja za Urad.

Okvir upravljanja s tveganji zajema naslednje elemente:

1. Periodična ocena tveganj varnosti informacijskih virov;
2. Presoja ustreznosti obstoječega kontrolnega okolja glede na oceno tveganj;
3. Obravnava tveganj— tveganja, ki so jim izpostavljeni informacijski viri Urada obravnavamo tako, da:
 - 🔑 uvedemo ali nadgradimo kontrolne aktivnosti, s katerimi zmanjšamo tveganje ali povečamo možnost, da bomo uresničeno tveganje pravočasno zaznali,
 - 🔑 jih zavestno sprejmemo ali
 - 🔑 se jim izognemo s tem, da prenehamo izvajati posamezno aktivnost, ki je povezana s tveganjem.

Sistem upravljanja s tveganji Urada zagotavlja kontinuirano nadgrajevanje notranje-kontrolnih aktivnosti za zaščito informacijskih virov Urada.

3 INFORMACIJSKI VIRI

3.1 Opis informacijskih virov

Informacijski viri Urada so:

- 🔑 **podatki in informacije:** vsi podatki ter informacije, ki se nahajajo v podatkovnih bazah, datoteke na strežnikih in delovnih postajah ter vsi podatki, ki se hranijo v fizični obliki, vključno s statističnimi podatki, rezultati statističnih obdelav, zbirkami osebnih podatkov, dokumentarnim in arhivskim gradivom, sistemsko dokumentacijo, uporabniški priročniki in navodili, vso dokumentacijo sistema varovanja informacij, pripadajoči pravilniki, ter druge informacije in podatki, ki se posredno ali neposredno uporabljajo pri delovanju Urada;
- 🔑 **programska oprema:** sistemska programska oprema, programska oprema, ki je namenjena statističnim obdelavam, vse aplikacijske rešitve in razvojna orodja;
- 🔑 **informacijska sredstva:** informacijska in komunikacijska oprema, nosilci podatkov ter druga tehnična oprema Urada;
- 🔑 **drugi informacijski viri:** uporabniška imena, gesla, sistemske nastavitve, administrativni viri in druge informacije ali zaupne informacije, do katerih Urad pridobi dostop pri svojem delovanju.

3.2 Skrbnik

Vsakemu informacijskemu viru se formalno imenuje vsebinskega in tehničnega skrbnika. Skrbništvo informacijskih virov mora biti dokumentirano in potrjeno s strani generalnega direktorja Urada.

Vsebinski skrbniki informacijskih virov klasificirajo informacijski vir in zahtevajo umestitev v varovano okolje. Tehnični skrbniki informacijskih virov so odgovorni za umestitev informacijskega vira v ustrezno varovano okolje.

Informacijski viri se smejo uporabljati le v skladu z namenom uporabe, ki je določen strani vsebinskega skrbnika informacijskega vira in potrjen s strani generalnega direktorja.

Kot ključne se določi vse tiste informacijske vire, ki jih na predlog OSUVI potrdi generalni direktor Urada.

3.3 Klasifikacija informacij

Urad je v »Pravilniku klasifikacije informacij« sprejel klasifikacijo informacij v skladu z notranjimi potrebami.

4 ORGANIZIRANOST VAROVANJA INFORMACIJ

4.1 Pristojnosti in odgovornosti

Generalni direktor:

- 🔑 seznanitev s periodičnimi pregledi in potrjevanje sprememb in dopolnitev krovne varnostne politike in vseh drugih pravilnikov s področja varovanja informacij;
- 🔑 zagotavljanje finančnih, človeških in organizacijskih virov za vpeljavo, vzdrževanje in nadgrajevanje sistema upravljanja varovanja informacij;
- 🔑 določitev ključnih informacijskih virov;
- 🔑 ocenjevanje učinkovitosti politike in ukrepov za varovanje informacij;
- 🔑 dodelitev vlog in odgovornosti s področja informacijske varnosti zaposlenim;
- 🔑 potrditev vpeljave programov internega izobraževanja in zviševanja osveščenosti na področju informacijske varnosti;
- 🔑 zagotavljanje usklajenosti aktivnosti in ukrepov varovanja informacijske varnosti v organizacijski strukturi Urada;
- 🔑 zagotavljanje skladnosti varovanja informacij z zakonodajo;
- 🔑 zagotavljanje skladnosti varovanja informacij s priporočili MJU.

Odbor za sistem upravljanja varovanja informacij (OSUVI):

- 🔑 razvoj strategije, ciljev in standardov varovanja informacij;
- 🔑 svetovanje generalnemu direktorju s področja varovanja informacij;
- 🔑 koordiniranje aktivnosti za vzpostavitev, vzdrževanje in nadgrajevanje sistema upravljanja varovanja informacij;
- 🔑 nadzor sistema upravljanja varovanja informacij;
- 🔑 predlaganje ključnih informacijskih virov;
- 🔑 poročanje generalnemu direktorju o stanju na področju varovanja informacij;
- 🔑 vodenje in poročanje generalnemu direktorju o postopkih za upravljanje varnostnih dogodkov;
- 🔑 periodičen pregled ter predlaganje sprememb in dopolnitev pravilnikov in postopkov informacijske varnosti;
- 🔑 aktivno sodelovanje pri odpravi škode, ki jo povzročijo incidenti, prekinitev delovanja in drugi dogodki, ki bi lahko ogrozili varnost informacijskih virov;
- 🔑 načrtovanje internih izobraževanj s področja informacijske varnosti;
- 🔑 obravnava vlog posameznikov pri uveljavljanju pravic na podlagi zakona, ki ureja varstvo osebnih podatkov,
- 🔑 usmerjanje aktivnosti za neprekinjeno delovanje Urada.

Podrobnejše naloge in odgovornosti OSUVI določa Poslovnik Odbora za sistem upravljanja varovanja informacij.

Odbor za varstvo podatkov (OVP):

- 🔑 skrb za izvajanje določb Pravilnika o postopkih in ukrepih za varstvo podatkov, zbranih s programom statističnih raziskovanj na Statističnem uradu Republike Slovenije;
- 🔑 obravnavanje zadev in svetovanje generalnemu direktorju o vprašanjih, ki jih ni mogoče rešiti s splošnimi pravili s področja varstva podatkov;
- 🔑 poročanje generalnemu direktorju in Statističnemu svetu Republike Slovenije o stanju na področju varstva podatkov v uradu;
- 🔑 druge naloge.

Podrobnejše naloge in odgovornosti OVP določa Poslovnik Odbora za varstvo podatkov.

Skrbnik informacijske varnosti:

- 🔑 razvoj in uvajanje tehnoloških rešitev na področju informacijske varnosti;
- 🔑 spremljanje in analiziranje stanja informacijske varnosti ter predlaganje ukrepov za izboljšanje OSUVI-ju;
- 🔑 poročanje o stanju na področju informacijske varnosti OSUVI-ju;
- 🔑 ocenitev vrednosti posameznih informacijskih virov skupaj z vsebinskim skrbnikom;
- 🔑 upravljanje tveganj s področja informacijske varnosti;
- 🔑 reševanje varnostnih incidentov;
- 🔑 nadzor fizičnih dostopov do IKT opreme;
- 🔑 nadzor nad dostopi do informacijskih virov;
- 🔑 upravljanje kakovosti izvajanja informacijske varnosti;
- 🔑 ocenjevanje skladnosti informacijske varnosti z zakonodajo in priporočili MJU;
- 🔑 spremljanje in uvajanje novosti na področju varnostnih nastavitev ter postopkov;
- 🔑 predlaganje in izvajanje aktivnosti za neprekinjeno delovanje;
- 🔑 poročanje in predlaganje sprememb na področju neprekinjenega delovanja Urada;
- 🔑 sodelovanje v razvojnih projektih ;
- 🔑 sodelovanje pri pripravi in izvajanju pogodb z zunanjimi izvajalci z vidika informacijske varnosti;
- 🔑 nadziranje zunanjih izvajalcev z vidika informacijske varnosti;
- 🔑 izobraževanje zaposlenih na področju ozaveščanja in izvajanja informacijske varnosti in neprekinjenega delovanja.

Vodja sektorja za informacijsko infrastrukturo in tehnologijo:

- 🔑 zagotavljanje ustreznega izvajanja tehnoloških in nekaterih organizacijskih ukrepov varovanja informacijskih virov;
- 🔑 aktivno sodelovanje v OSUVI.

Vodja službe, pristojne za splošne zadeve:

- 🔑 zagotavljanje ustreznega izvajanja tehničnih in nekaterih organizacijskih ukrepov varovanja informacijskih virov;
- 🔑 aktivno sodelovanje v OSUVI.

Vsebinski skrbnik informacijskih virov:

- 🔑 klasificiranje informacijskega vira in zahtevanje njegove umestitve v ustrezno informacijsko okolje;
- 🔑 podajanje zahtev tehničnemu skrbniku za dodeljevanje uporabniških pravic in izvajanje nadzora nad dodeljenimi uporabniškimi pravicami;
- 🔑 prepoznavanje in ocenitev tveganj, ki izhajajo iz nepooblaščenega dostopa do informacijskih virov katerih skrbniki so;
- 🔑 preprečevanje razkritja podatkov, ki jih je pripravil za objavo, pred datumom objave in zagotavljanje statistične zaščite za diseminirane podatke.

Tehnični skrbnik informacijskih virov:

- 🔑 zagotavljanje in vzdrževanje ustreznega varnostnega okolja, v katero je umeščen informacijski vir;
- 🔑 dodeljevanje pravic dostopa do informacijskih virov na podlagi zahtevka vsebinskega skrbnika informacijskega vira;
- 🔑 preventivno delovanje na področju informacijske varnosti;
- 🔑 aktivno odpravljanje škode ob incidentih;
- 🔑 obveščanje OSUVI o zaznanih varnostnih grožnjah.

Vodje notranje organizacijske enote:

- 🔑 izvajanje postopkov in ukrepov za zavarovanje osebnih podatkov.

Zaposleni, pogodbeni sodelavci, zunanji izvajalci in druge osebe, ki pridobijo dostop do informacijskih virov Urada:

- 🔑 spoštovanje določil in varnostnih standardov, določenih s to politiko in drugimi pravilniki informacijske varnosti;
- 🔑 obdelovanje podatkov v ustreznem varnostnem okolju (podatkovni in datotečni strežniki v primeru elektronske obdelave, v primeru ročne obdelave v skladu s Pravilnikom o ravnanju uslužbencev za zagotavljanje informacijske varnosti);
- 🔑 preprečevanje razkritja podatkov pripravljenih za objavo pred datumom objave in zagotavljanje statistične zaščite za diseminirane podatke;
- 🔑 obveščanje o zaznanih varnostnih incidentih;
- 🔑 uporaba informacijskih virov zgolj v skladu s predpisanim namenom uporabe;
- 🔑 udeležba na izobraževanju o informacijski varnosti v skladu z izobraževalnim programom Urada.

5 KONČNE DOLOČBE

OSUVI izvaja redne letne pregleda te krovne varnostne politike in jo po potrebi uskladi z drugimi pravilniki in politikami Urada ali prilagodi potrebam Urada.

Ta krovna varnostna politika začne veljati trideseti dan po objavi na internem portalu Urada.

Številka: 007-47/2011/1

Datum: 21. 9. 2011



Križman
Mag. Irena Križman,
generalna direktorica

PRILOGA 1: Izjava o seznanitvi s politiko varovanja informacij in podrejenimi področnimi pravilniki

Spodaj podpisani _____,

rojen dne _____, v _____, izjavljam:

☞ da sem prejel izvod:

- ✓ Izvlečka o osnovnih aktivnosti zaposlenih na področju varovanja informacij na Statističnem uradu Republike Slovenije;
- ✓ Politike varovanja informacij Statističnega urada Republike Slovenije;
- ✓ Pravilnika o varstvu osebnih podatkov zaposlenih na Statističnem uradu Republike Slovenije;
- ✓ Izjave o varstvu osebnih podatkov;
- ✓ Pravilnika o varstvu podatkov, zbranih s programom statističnih raziskovanj na Statističnem uradu Republike Slovenije;
- ✓ Izjave o varstvu podatkov zbranih s programom statističnih raziskovanj;
- ✓ Pravilnika o ravnanju zaposlenih za zagotavljanje informacijske varnosti;
- ✓ Pravilnika o uporabi interneta;
- ✓ Pravilnika o uporabi elektronske pošte;
- ✓ Pravilnika o dodeljevanju in nadzoru uporabniških dostopov;
- ✓ Pravilnika o uporabi prenosne komunikacijske in računalniške opreme ter oddaljenemu dostopu,
- ✓ Pravilnika o zaščiti pred zlonamerno programsko opremo;
- ✓ Pravilnika o naročanju storitev informacijsko komunikacijske tehnologije pri zunanjih izvajalcih, ki vstopajo v informacijski sistem Statističnega urada Republike Slovenije;
- ✓ Pravilnika o klasifikaciji informacij;
- ✓ Pravilnika o postopkih za upravljanje varnostnih dogodkov;

☞ da sem dokumente v celoti prebral;

☞ da razumem vsa njihova določila in njihov pomen in se zavezujem, da bom spoštoval vsa določila, navedena v njih;

☞ da se zavedam, da je kršitev politike varovanja informacij in pravilnikov podlaga za izvajanje in uvedbo sankcij, določenih s temi pravilniki, drugimi notranjimi akti Urada ter veljavno zakonodajo Republike Slovenije.

V _____, dne _____

Ime in priimek:

Podpis:
