Politika varovanja informacij Statističnega urada Republike Slovenije

Zgodovina sprememb:

Verzija	Datum	Številka dokumenta
1	21.9.2011	007-47/2011/1
2	24.4.2015	007-47/2011/26
3	29.11.2017	007-47/2017/1
4	18.10.2018	007-47/2017/20

VSEBINA

Na podlagi drugega odstavka 42. člena Zakona o državni statistiki (Uradni list RS, št. 45/95 in 9/01) ter v skladu s prvim odstavkom 80. člena Uredbe o upravnem poslovanju (Uradni list RS, št. 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07, 31/08, 35/09, 58/10, 101/10 in 81/13) generalna direktorica Statističnega urada Republike Slovenije izdaja naslednjo

Politiko varovanja informacij Statističnega urada Republike Slovenije

1. NAMEN IN CILJI POLITIKE VAROVANJA INFORMACIJ

Namen Politike varovanja informacij je vzpostavitev celostnega sistema upravljanja varovanja informacij (SUVI) in podatkov v Statističnem uradu Republike Slovenije (v nadaljevanju: SURS), s ciljem zagotavljanja delovanja SURS 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 SURS ter zagotavljanje njegovega neprekinjenega delovanja. 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 na SURS - ti morajo poznati in ravnati v skladu z ustrezno zakonodajo in vsemi notranjimi pravili s področja varovanja informacij.

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

2. OBSEG IN TEMELJNA NAČELA VAROVANJA INFORMACIJ

2.1 Obseg

Ta krovna politika varovanja informacij predstavlja osnovni dokument upravljanja varovanja informacij in podatkov na SURS. Določa splošne smernice in načela varovanja informacij in podatkov SURS, nanaša pa se na vse informacijske vire SURS. Skupaj s pravilniki, navodili in drugimi dokumenti, sprejetimi v njenem okviru (v nadaljevanju: politika varovanja informacij), predstavlja formalni okvir sistema upravljanja varovanja informacij na SURS.

Namenjena je zaposlenim na SURS, pogodbenim sodelavcem, zunanjim izvajalcem ter vsem drugim osebam, ki pridobijo dostop do informacijskih virov SURS (v nadaljevanju: uporabniki). Vsi našteti so odgovorni za spoštovanje te politike in drugih pravilnikov informacijske varnosti ter za spoštovanje organizacijskih in tehničnih ukrepov, ki se navezujejo na varovanje informacij na SURS.

2.2 Načela

Celostni sistem upravljanja varovanja informacij na SURS je zasnovan na priporočilih standarda informacijske varnosti ISO 27001:2013 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 predpisi informacijske varnostne politike Ministrstva za javno upravo.

Vsak uporabnik 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 pravilnikov varovanja informacij nadrejenim oz. skrbniku informacijske varnosti.

Vsak uporabnik mora biti pred začetkom opravljanja dela na SURS seznanjen s politiko varovanja informacij ter z dolžnostmi in odgovornostmi v povezavi z varovanjem informacij. Prav tako mora biti vsak uporabnik na SURS formalno zavezan k spoštovanju politike varovanja informacij. Obrazec izjave, ki jo mora podpisati vsaka oseba, ki s SURS 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 na SURS. 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 SURS.

Dejanja, ki so v nasprotju z načeli varovanja informacij SURS, predstavljajo kršitev delovnih obveznosti. Kršitve se smatrajo kot kršitve pogodbe o zaposlitvi oziroma druge pogodbe, ki ureja pravni odnos, na podlagi katerega oseba pridobi dostop do informacijskih virov SURS. 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.

SURS 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.

Politika varovanja informacij je predmet periodičnega pregleda. Politika varovanja informacij se dopolnjuje in razvija skladno z dejanskimi potrebami SURS. Viri informacij za dopolnitev in nadgradnjo so lahko:

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

O spremembah krovne varnostne politike in posameznih področnih pravilnikov se vsakokrat seznani vse uporabnike SURS preko službene e-pošte in z objavo na intranetu oziroma na drug ustrezen način.

2.3. Dokumenti informacijske varnosti

Sistem upravljanja varovanja informacij SURS je zastavljen v obliki varnostnih pravilnikov, navodil, operativnih postopkov in smernic. Krovna politika varovanja informacij predstavlja osnovni dokument za organizacijo varovanja informacij na SURS. 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, varnostne mehanizme in nivo njihovega varovanja, ustrezno uporabo posameznih virov ter odgovornosti in vloge posameznih uporabnikov pri upravljanju teh virov;
- **Navodila,** ki natančneje opredeljujejo ravnanje uporabnikov;

- **Operativni postopki,** ki vsebujejo natančna pravila o ravnanju z informacijskimi viri;
- **Smernice,** ki so skupki pravil za določeno skupino informacijskih virov ali za določeno skupino uporabnikov.

2.4. Kontrolno okolje in upravljanje s tveganji

Ukrepi varovanja informacijskih virov SURS 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 SURS.

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 SURS 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 SURS zagotavlja kontinuirano nadgrajevanje notranje-kontrolnih aktivnosti za zaščito informacijskih virov SURS.

2.5 Izvajanje notranjih presoj

Z namenom ugotavljanja uspešnosti in učinkovitosti vpeljanega sistema upravljanja varovanja informacij se vsaj enkrat letno izvede notranja presoja izvajanja postopkov in ukrepov varovanja informacij.

Notranje presoje izvaja skupina presojevalcev, imenovanih s strani generalnega direktorja za izvedbo posamezne presoje. V skupino se lahko imenujejo zaposleni, ki so pridobili potrdilo o usposobljenosti za notranjega presojevalca sistema upravljanja informacijske varnosti. Notranjo presojo vodi skrbnik informacijske varnosti v vlogi vodilnega presojevalca, ki je pridobil potrdilo o usposobljenosti za vodilne presojevalce sistema upravljanja informacijske varnosti.

Vodilni presojevalec pripravi predlog programa presoj prihodnjega leta do 31.12. tekočega leta.

Pri izvajanju notranjih presoj mora biti zagotovljeno, da presojevalci ne opravljajo presoje na področjih, za katere so odgovorni.

Vodilni presojevalec po opravljeni presoji pripravi poročilo o presoji ter seznani generalnega direktorja z rezultati presoje. Na podlagi rezultatov presoje skrbnik informacijske varnosti pripravi predlog ukrepov. Sistem presoj zagotavlja kontinuirano izboljševanje informacijske varnosti.

3. INFORMACIJSKI VIRI

3.1 Opis informacijskih virov

Informacijski viri SURS 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 SURS;
- **programska oprema:** sistemska programska oprema, programska oprema, ki je namenjena statističnim obdelavam, vse aplikacijske rešitve in razvojna orodja;
- **informacijska sredstva:** informacijska in komunikacijska infrastruktura, nosilci podatkov ter druga tehnična oprema SURS;
- **drugi informacijski viri:** uporabniška imena, gesla, sistemske nastavitve, administrativni viri in druge informacije ali zaupne informacije, do katerih SURS 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.

4. ORGANIZIRANOST VAROVANJA INFORMACIJ

4.1 Vloge in odgovornosti

Generalni direktor:

- seznanitev s periodičnimi pregledi stanja sistema in potrjevanje sprememb in dopolnitev dokumentov politike varovanja informacij;
- zagotavljanje finančnih, človeških in organizacijskih virov za vpeljavo, vzdrževanje in nadgrajevanje sistema upravljanja varovanja informacij;
- seznanitev z rezultati presoj izvajanja postopkov in ukrepov varovanja informacij;
- ocenjevanje učinkovitosti politike in ukrepov za varovanje informacij;
- dodelitev vlog in odgovornosti s področja varovanja informacij uporabnikom;
- potrditev vpeljave programov internega izobraževanja in zviševanja osveščenosti na področju informacijske varnosti;
- zagotavljanje usklajenosti aktivnosti in ukrepov varovanja informacij v organizacijski strukturi SURS;
- zagotavljanje skladnosti varovanja informacij z zakonodajo;
- zagotavljanje skladnosti varovanja informacij s predpisi MJU.

Skrbnik informacijske varnosti:

- preverjanje skladnosti informacijske varnosti z zakonodajo, s skupnim okvirjem informacijske varnosti Evropskega Statističnega Sistema, s predpisi informacijske varnosti MJU ter z ostalimi standardi informacijske varnosti;
- periodičen pregled ter vzdrževanje politik, standardov in navodil s področja informacijske varnosti in predlaganje sprememb in dopolnitev;
- koordiniranje aktivnosti za vzdrževanje in nadgrajevanje sistema upravljanja varovanja informacij;
- svetovanje generalnemu direktorju s področja varovanja informacij;
- spremljanje in uvajanje novosti na področju varnostnih mehanizmov ter postopkov;
- upravljanje tveganj informacijske varnosti;
- spremljanje izvajanja določil politik in navodil na področju informacijske varnosti;
- upravljanje in obravnava varnostnih dogodkov;
- aktivno sodelovanje pri odpravi škode, ki jo povzročijo varnostni dogodki, prekinitve delovanja in drugi dogodki, ki bi lahko ogrozili varnost informacijskih virov;
- predlaganje in usmerjanje aktivnosti za neprekinjeno delovanje;
- poročanje in predlaganje sprememb na področju neprekinjenega delovanja;

- nadzor fizičnih dostopov do IKT opreme ter oddaljenih dostopov do informacijskega sistema SURS;
- pregledovanje revizijskih sledi;
- sodelovanje v razvojnih projektih z namenom zagotavljanja vidika informacijske varnosti;
- sodelovanje pri upravljanju s spremembami, ki so povezane z upravljanjem informacijskega sistema ali z informacijsko varnostjo;
- 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;
- priprava letnega poročila o stanju na področju varovanja informacij ter o varnostnih dogodkih;
- redno poročanje generalnemu direktorju.

Varnostni forum:

- svetovanje in zagotavljanje podpore ter informacij skrbniku informacijske varnosti pri pripravi politik, standardov in navodil s področja informacijske varnosti ter pri ostalih aktivnostih in postopkih informacijske varnosti.

Odbor za statistično zaupnost (OSZ):

- priprava analize in predloga odločitve v zvezi z dostopom do zaupnih podatkov pod posebnimi pogoji (znanstveno – raziskovalni namen);
- priprava analize in predloga odločitve v zvezi s posredovanjem osebnih podatkov za anketiranje zunanjim uporabnikom;
- obravnava zadev in svetovanje v zvezi z varovanjem statistične zaupnosti zaposlenih in drugih oseb, ki pridobijo dostop do zaupnih podatkov;
- obravnava zadev in svetovanje glede uporabe zaupnih podatkov za statistični namen;
- obravnava zadev in predlaganje odločitev v zvezi s prošnjami enot, ki zaprosijo za dostop do individualnih podatkov, ki se nanašajo nanje ali so jih le te posredovale SURS;
- obravnava prošenj in predlaganje odločitev v zvezi s prošnjami institucij ali drugih subjektov, ki zaprosijo za dostop do zaupnih podatkov z namenom uporabe le teh za določanje pravic in obveznostim enotam, na katere se zaupni podatki nanašajo;
- obravnava zadev in svetovanje z vidika objavljanja podatkov in enakopravnega dostopa uporabnikov;
- obravnava in svetovanje glede drugih zadev, ki se nanašajo ali so v povezavi z varovanjem statistične zaupnosti.

Vodja sektorja za informacijsko infrastrukturo in tehnologijo:

- zagotavljanje ustreznega izvajanja potrebnih tehnoloških in organizacijskih ukrepov varovanja informacijskih virov;
- aktivno sodelovanje v varnostnem forumu.

Vodja službe, pristojne za splošne zadeve:

- zagotavljanje ustreznega izvajanja potrebnih tehničnih in organizacijskih ukrepov varovanja informacijskih virov.

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;

- prepoznava in ocenitev tveganj, ki izhajajo iz nepooblaščenega dostopa do informacijskih virov katerih skrbniki so;
- preprečevanje razkritje 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 varnostnih dogodkih;
- obveščanje skrbnika informacijske varnosti o zaznanih varnostnih grožnjah.

Vodje notranje organizacijskih enot:

- izvajanje postopkov in ukrepov varovanja informacij.

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

- spoštovanje določil in varnostnih standardov, določenih s politiko varovanja informacij;
- obdelovanje podatkov v ustreznem varnostnem okolju;
- preprečevanje razkritja podatkov pripravljenih za objavo pred datumom objave in zagotavljanje statistične zaščite na podatkih, namenjenih za objavo;
- obveščanje o zaznanih varnostnih incidentih;
- uporaba informacijskih virov v skladu s predpisanim namenom uporabe;
- udeležba na izobraževanjih o informacijski varnosti.

5. KONČNI DOLOČBI

Ta krovna politika varovanja informacij začne veljati naslednji dan po objavi na internem portalu SURS.

Z dnem začetka veljavnosti te krovne politike varovanja informacij preneha veljati Politika varovanja informacij Statističnega urada Republike Slovenije št. 007-47/2017/1 z dne 29. 11. 2017.

Številka: 007-47/2017/20
Datum: 18. 10. 2018

Genovefa Ružić,
v. d. generalne direktorice

PRILOGA

REPUBLIKA SLOVENIJA
STATISTIČNI URAD RS

SURS Litostrojska cesta 54, 1000 Ljubljana, Slovenija

Izjava o seznanitvi s celovito politiko varovanja informacij

Spodaj podpisani _____ ,

rojen dne _____, v _____, izjavljam:

- da sem prejel izvod:
  - ✓ Politike varovanja informacij Statističnega urada Republike Slovenije;
  - ✓ Pravilnika o varstvu osebnih podatkov zaposlenih;
  - ✓ Pravilnika o varstvu podatkov zbranih s programom statističnih raziskovanj na Statističnem uradu Republike Slovenije;
  - ✓ Pravilnika o ravnanju uporabnikov za zagotavljanje informacijske varnosti;
  - ✓ Pravilnika o uporabi interneta;
  - ✓ Pravilnika o uporabi elektronske pošte;
  - ✓ Pravilnika o upravljanju informacijskega sistema;
  - ✓ 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 SURS;
  - ✓ Pravilnika o klasifikaciji informacij;
  - ✓ Pravilnika o postopkih za upravljanje varnostnih dogodkov;
  - ✓ Pravilnika o upravljanju s spremembami;
  - ✓ Pravilnika o upravljanju neprekinjenega delovanja.

- 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 podlaga za izvajanje in uvedbo sankcij, določenih s temi pravilniki, drugimi notranjimi akti SURS ter veljavno zakonodajo Republike Slovenije.

V _____, dne _____

Ime in priimek:

_____

Podpis:

_____