

## Pravilnik o upravljanju informacijskega sistema

### Zgodovina sprememb:

Verzija	Datum	Številka dokumenta
1	29.11.2017	007-47/2017/5
2	5.10.2022	007-47/2017/31

Na podlagi drugega odstavka 42. člena Zakona o državni statistiki (Ur. list RS, št. 45/1995, 9/2001) ter v skladu z Uredbo o informacijski varnosti v državni upravi (Uradni list RS, št. 29/18, 131/20) predstojnik Statističnega urada Republike Slovenije izdaja naslednji

## **Pravilnik o upravljanju informacijskega sistema**

### **1 SPLOŠNE DOLOČBE**

#### **1.1 Namen**

Pravilnik določa postopke in ukrepe, povezane z upravljanjem informacijskega sistema Statističnega urada Republike Slovenije (v nadaljevanju: SURS), z razvojem informacijskih rešitev in upravljanjem uporabniške informacijsko komunikacijske opreme SURS.

#### **1.2 Cilj**

Cilj pravilnika je učinkovito zagotavljanje informacijske varnosti s strani oseb, ki upravljajo (v nadaljevanju: tehnični skrbniki) informacijski sistem oziroma systemske informacijske vire SURS.

#### **1.3 Predmet**

Pravilnik se nanaša na informacijski sistem SURS, ki je skupek med seboj odvisnih komponent računalniške strojne, programske in komunikacijske opreme. Posamezne komponente informacijskega sistema so systemski informacijski viri.

Med systemske informacijske vire spada predvsem strežniška strojna oprema, diskovna polja, sistemi za varnostno kopiranje, virtualni strežniki, systemska programska oprema, omrežna in komunikacijska oprema.

### **2 UPRAVLJANJE INFORMACIJSKEGA SISTEMA**

#### **2.1 Splošno**

Z namenom pravilnega in varnega izvajanja nalog tehničnih skrbnikov in uporabnikov informacijskega sistema SURS, morajo biti za vsak systemski informacijski vir izdelana operativna navodila, v katerih so opisani postopki za namestitve, vzdrževanje, varnostno kopiranje, obnovo sistema in druge informacije, ki zagotavljajo zanesljivo in varno delovanje in upravljanje informacijskega sistema. Operativna navodila morajo biti izdelana pred prenosom systemskega informacijskega vira v produkcijsko okolje in biti na voljo vsem uporabnikom, ki jih potrebujejo. Za pripravo operativnih navodil je odgovoren tehnični skrbnik posameznega systemskega informacijskega vira. Operativna navodila vsebujejo informacije, katerih razkritje bi SURS izpostavilo zunanjim grožnjam in so klasificirana v klasifikacijski razred občutljivo, zato morajo biti hranjena na način, da niso dostopna nepooblaščenim osebam.

Systemski informacijski viri informacijskega sistema SURS morajo biti nastavljeni tako, da se njihova ura redno sinhronizira z univerzalnim koordiniranim časom preko protokola ntp (Network Time Protocol).

V informacijskem sistemu SURS se sme uporabljati izključno nelicenčna programska oprema ali programska oprema z urejenimi licenčnimi pravicami.

Tehnični skrbniki so zadolženi za redno spremljanje informacij in strokovne literature o novih ranljivostih njihovih sistemov. Tehnični skrbniki so zadolženi za preglede, preventivno vzdrževanje in redno posodabljanje systemskih informacijskih virov v skladu z dobro prakso in navodili proizvajalcev.

Vse izvedene preglede in posege morajo dokumentirati.

Kakršne koli spremembe v informacijskem sistemu SURS, ki vplivajo na njegovo funkcionalnost ali varnost, morajo biti izvedene v skladu s Pravilnikom o upravljanju s spremembami.

Administratorski dostopi za sistemske informacijske vire se morajo upravljati v skladu s Pravilnikom o dodeljevanju in nadzoru uporabniških dostopov.

## **2.2 Navodila za upravljanje strojne strežniške opreme**

Strojna strežniška oprema je nameščena v varnem podatkovnem centru, kamor je dostop omogočen izključno pooblaščenim tehničnim skrbnikom. Strojno strežniško opremo morajo tehnični skrbniki vsaj enkrat tedensko pregledovati in jo vzdrževati po priporočilih proizvajalca, preglede pa dokumentirati. Vsa strojna oprema v varnem podatkovnem centru mora biti ustrezno označena z nazivom opreme, ki mora biti unikatna in smiselno opisan ter brez presledkov. Naziv se prilepi na vidno mesto na strojno opremo. Skladno se označi tudi kable (omrežne, optične, električne, KVM). Kabli morajo biti razločno in z enakimi oznakami označeni na obeh straneh. Kabli morajo biti označeni tudi v telekomunikacijskih omarah v varnem podatkovnem centru, kjer so priključeni na aktivno omrežno opremo.

## **2.3 Navodila za upravljanje omrežja**

Dostop do aktivne omrežne opreme je omogočen izključno pooblaščenim tehničnim skrbnikom. Vsi omrežni priključki, ki niso v uporabi, morajo biti onemogočeni.

Informacijski sistem SURS je zaščiten pred vdori s sistemom požarnih pregrad. V omrežju je vzpostavljena demilitarizirana varna cona (DMZ) s strežniki, ki so dostopni iz interneta. Vse poti med notranjim omrežjem SURS in DMZ so nadzorovane.

Za goste je vzpostavljeno posebno brezžično omrežje, ki omogoča gostom dostop do interneta brez povezave z informacijskim sistemom SURS.

Kakršne koli spremembe v povezavi z upravljanjem omrežja ter požarne pregrade morajo biti izvedene v skladu s Pravilnikom o upravljanju s spremembami.

# **3 Razvoj informacijskih rešitev**

## **3.1 Splošno**

Pri razvoju informacijskih rešitev SURS je potrebno izvajati naslednje ukrepe:

- \* varnostne zahteve je potrebno določiti in uvesti kot del sistemskih zahtev, upoštevati je potrebno Zahteve in dobre prakse za razvoj varnih aplikacij in njihovo uporabo ustrezno dokumentirati,
- \* informacijsko varnost je potrebno upoštevati v vseh fazah razvojnega cikla, za sistematično zmanjševanje varnostnih ranljivosti informacijskih rešitev je potrebno izvajati aktivnosti za preprečevanje varnostnih ranljivosti informacijskih rešitev,
- \* informacijske rešitve morajo biti ustrezno dokumentirane,
- \* pred namestitvijo informacijske rešitve v produkcijo je potrebno informacijsko rešitev varnostno pregledati in testirati, ugotovitve dokumentirati, ter preveriti konfiguracijo programskega in systemskega okolja skladno s Pravilnikom o upravljanju s spremembami.

### **3.2 Preprečevanje varnostnih ranljivosti informacijskih rešitev**

Vse osebe, ki sodelujejo pri razvoju informacijskih rešitev SURS, morajo upoštevati Zahteve in dobre prakse za razvoj varnih aplikacij na naslednjih področjih:

- \* Analiza varnostnih zahtev aplikacije
- \* Analiza skladnosti
- \* Načrtovanje varne arhitekture aplikacije
- \* Razvoj varne programske kode
- \* Generične Tehnološke Zahteve za razvoj informacijskih sistemov v okolju MJU
- \* Razvoj varnih spletnih storitev
- \* Validacija vnosnih podatkov
- \* Varnostni pregled in analiza programske kode
- \* Penetracijsko testiranje
- \* Namestitev aplikacije v produkcijo
- \* Vzpostavitev izvajalnih okolij
- \* Varnostni pregled izvajalnega okolja

### **3.3 Uporaba sistemov za upravljanje izvirne kode**

Pri razvoju programske opreme se uporablja sistem za verzioniranje kode. Za vsako namestitev novega modula ali popravka obstoječega modula mora razvijalec pripraviti ustrezna navodila za namestitev in prenesti izvirno kodo v sistem za upravljanje izvirne kode.

Nove verzije in popravki aplikacij se vedno najprej namestijo na testno okolje.

Odgovorni razvijalec opravi najmanj naslednja preverjanja, da:

- \* je bila namestitev opravljena v skladu s spremenjenimi zahtevami,
- \* informacijska rešitev deluje v skladu s funkcionalnimi in varnostnimi zahtevami,
- \* je informacijska rešitev tudi performančno ustrezna in deluje v skladu s pričakovanji;

### **3.4 Prenos v produkcijo**

Za vsako informacijsko rešitev je potrebno vzpostaviti najmanj 2 izvajalni okolji: testno in produkcijsko:

- \* testno okolje služi potrditvenemu testiranju (tudi preverjanju, ali je bil nek popravek izveden v skladu z funkcionalnimi in varnostnimi zahtevami,
- \* produkcijsko služi polni produkciji. Nameščajo se samo popravki, katerih prehod iz testa na produkcijo je bil odobren v skladu s pravilnikom za upravljanje sprememb.

Programska oprema se razvija izključno v razvojnem okolju. Ko so funkcionalnosti implementirane in se smatrajo, da so stabilne, se prenesejo v testno okolje. Ko se informacijska rešitev prenese v testno okolje se obvesti vsebinskega skrbnika. Vsebinski skrbnik preveri delovanje novih funkcionalnosti in potrdi pravilno delovanje.

Ko se funkcionalnost informacijske rešitve uspešno stestira v testnem okolju, se lahko prenese v produkcijsko okolje.

Prenos v produkcijo se izvaja samo ob večjih spremembah informacijske rešitve in v času, ko se le ta najmanj uporablja ter v skladu s Pravilnikom o upravljanju sprememb.

### **3.5 Podatki v razvojnih in testnih okoljih**

V razvojnih in testnih okoljih je potrebno uporabljati testne podatke, ki v skladu s Pravilnikom o klasifikaciji informacij niso klasificirani kot občutljivi ali interni.

#### 4 Upravljanje uporabniške IKT opreme

Med uporabniško IKT opremo spadajo delovne postaje, računalniški monitorji, prenosni računalniki, tablični računalniki, tiskalniki ter ostala IKT oprema, ki jo pri svojem delu neposredno uporabljajo uporabniki.

Z uporabniško IKT opremo SURS je potrebno ravnati gospodarno. Evidenco z uporabniško IKT opremo, ki vsebuje podatke o posameznih elementih (tip, inventarna številka, nadgradnje, uporabnik), vodi in vzdržuje organizacijska enota, pristojna za infrastrukturo in tehnologijo. Evidenca mora odražati dejansko stanje dodeljene opreme uporabnikom.

Uporabniška IKT oprema se uporabnikom dodeljuje izključno na podlagi pisne zahteve ob okvari obstoječe opreme ali ob potrebi po zmogljivejši opremi. Predlog razdelitve uporabniške IKT opreme se pripravi v službi, pristojni za infrastrukturo na podlagi utemeljenih prejetih zahtev vodij sektorjev in služb. V primeru, ko je zahtevkov ob nakupu opreme več, kot je na voljo opreme, se zahtevki realizirajo glede na tip zahteve, ki imajo različne prioritete.

- \* Prioriteta 1: Zdravstveni razlogi (npr. ustrezen monitor zaradi slabega vida - zdravniško potrdilo)
- \* Prioriteta 2: Strojne zahteve za delovanje potrebne programske opreme
- \* Prioriteta 3: Konfiguracija obstoječe opreme uporabnika (starost/omejena uporabnost opreme)

V kolikor se je potrebno odločati med zahtevami istega prioritetnega razreda, imajo prednost uporabniki, ki uporabljajo manj zmogljivo opremo.

Delovne postaje SURS morajo biti nameščene v skladu s konfiguracijo »standardna delovna postaja«. Konfiguracija »standardna delovna postaja« pomeni utrjeno standardizirano operativno okolje s predpisanim operacijskim sistemom, pisarniškim paketom, odjemalcem elektronske pošte in drugo programsko opremo. Nastavljena mora biti tako, da ne vsebuje nepotrebne programske opreme in nepotrebnih uporabniških računov, onemogočene ali odstranjene so nepotrebne funkcije oziroma storitve. Odstopanja od »standardne delovne postaje« so dovoljena le za uporabnike, ki drugačno konfiguracijo nujno potrebujejo za učinkovito opravljanje dela in morajo biti odobrene s strani skrbnika informacijske varnosti ter za namenske delovne postaje, kot so tiste v anketnem studiu, varni sobi, računalniški učilnici.

Kakršne koli spremembe konfiguracije »standardne delovne postaje« smejo biti izvedene izključno v skladu s Pravilnikom o upravljanju s spremembami.

Tehnični skrbniki uporabniške IKT opreme so zadolženi za redno in sprotno nameščanje varnostnih popravkov v skladu s priporočili in dobrimi praksami. Nameščanje varnostnih popravkov mora biti dokumentirano.

Tehnični skrbniki uporabniške IKT opreme nameščajo programsko opremo na uporabniško IKT opremo ter izvajajo spremembe obstoječe programske opreme izključno na podlagi pisnega zahtevka vodij notranje organizacijskih enot. Na uporabniški IKT opremi SURS se sme uporabljati izključno programska oprema z urejenimi licenčnimi pravicami. Uporabniška IKT oprema SURS mora biti nastavljena tako, da je informacijska varnost zagotovljena v največji možni meri, kar pomeni predvsem uporabo mehanizmov:

- \* zaklepanje BIOSa;
- \* centralno upravljanje z varnostnimi popravki;
- \* enkripcija trdega diska pri prenosnih napravah;
- \* uporabniki nimajo administratorskih pravic, razen v izjemnih primerih, ki so urejeni v skladu s Pravilnikom o dodeljevanju in nadzoru uporabniških dostopov;
- \* centralno upravljanje protivirusne programske opreme v skladu s Pravilnikom o zaščiti pred zlonamerno programsko opremo;
- \* centralno upravljanje s prenosnimi nosilci podatkov v skladu s Pravilnikom o uporabi prenosne komunikacijske in računalniške (IKT) opreme in dostopu z daljave.

Pred ponovno uporabo uporabniške IKT opreme so tehnični skrbniki uporabniške IKT opreme dolžni

izbrisati vse morebitne podatke prejšnjih uporabnikov opreme.

V kolikor uporabniška IKT oprema, na kateri se nahajajo podatki, ki so v skladu s Pravilnikom o klasifikaciji informacij opredeljeni kot občutljivi ali interni, zapusti varovane prostore SURS, je potrebno pred tem odstraniti nosilce podatkov oziroma poskrbeti za preprečevanje nepooblaščenega dostopa do teh podatkov z izbrisom podatkov ali z uporabo enkripcije.

Pred odpisom računalniške opreme morajo tehnični skrbniki odstraniti podatkovne nosilce, jih do uničenja hraniti tako, da so zavarovani pred nepooblaščenim dostopom ter poskrbeti za popolno uničenje pod nadzorom pooblaščenih oseb v skladu z Navodilom za uničenje fizičnih dokumentov in elektronskih nosilcev podatkov.

## **5 KONČNA DOLOČBA**

Ta pravilnik začne veljati petnajsti dan po objavi na internem portalu SURS.

Z dnem začetka veljavnosti tega pravilnika preneha veljati Pravilnik o upravljanju informacijskega sistema št. 007-47/2017/5 z dne 29. 11. 2017.

Številka: 007-47/2017/31

Datum: 5. 10. 2022

Tomaž Smrekar,  
generalni direktor