

879

Na temelju članka 56. stavka 2. Zakona o državnoj izmjeri i katastru nekretnina (»Narodne novine«, br. 112/18 i 39/22), glavni ravnatelj Državne geodetske uprave donosi

ODLUKU

O STAVLJANJU U SLUŽBENU UPORABU KATASTARSKOG OPERATA KATASTRA NEKRETNINA ZA KATASTARSKU OPĆINU VELIKA VES NOVA

I.

Na temelju podataka elaborata katastarske izmjere, podataka prikupljenih tijekom izlaganja na javni uvid elaborata katastarske izmjere i podataka preuzetih iz obnovljene zemljišne knjige, izrađen je katastarski operat katastra nekretnina za katastarsku općinu Velika Ves Nova (MB 338702), a koji se sastoji od:

- katastarskog plana u digitalnom obliku
- elaborata geodetske osnove
- pregledne karte u mjerilu 1:8500 s podjelom na detaljne listove katastarskog plana te podjelom na skice izmjere
- detaljnih listova katastarskog plana u mjerilu 1:1000 (50 listova)
- skica izmjere mjerila 1:1000 (50 komada)
- dopunskih skica izmjere raznih mjerila (135 komada)
- popisa katastarskih čestica u rasponu od broja 1 do 2782 (ukupno 2805 k.č.)
- popisa osoba upisanih u posjedovne listove i
- posjedovnih listova u rasponu od broja 1 do 2076 (ukupno 1711 PL-ova).

II.

Katastarski operat katastra nekretnina za katastarsku općinu Velika Ves Nova (MB 338702), stavlja se u službenu uporabu dana 11. svibnja 2023. godine.

III.

Od dana stavljanja u službenu uporabu katastarskog operata katastra nekretnina za katastarsku općinu Velika Ves Nova (MB 338702) svi novi upisi na području na kojem je provedena katastarska izmjera provoditi će se u katastarskom operatu katastra nekretnina za katastarsku općinu Velika Ves Nova (MB 338702).

IV.

Katastarski operat katastra nekretnina za katastarsku općinu Velika Ves Nova (MB 338702) mora se održavati u trajnoj suglasnosti s novoosnovanom zemljišnom knjigom za katastarsku općinu Velika Ves.

V.

Ova Odluka stupa na snagu danom donošenja i objavit će se u »Narodnim novinama«.

Klasa: 932-05/23-03/3
Urbroj: 541-04-01-02/4-23-4
Zagreb, 9. svibnja 2023.

Glavni ravnatelj
Antonio Šustić, dipl. ing. geod., v. r.

DRŽAVNI ZAVOD ZA STATISTIKU

880

Državni zavod za statistiku objavljuje

INDEKS

PROIZVOĐAČKIH CIJENA INDUSTRIJSKIH PROIZVODA NA DOMAĆEM TRŽIŠTU U TRAVNJU 2023.

Indeks proizvođačkih cijena industrijskih proizvoda na domaćem tržištu u travnju u travnju 2023. u odnosu na ožujak 2023. iznosi **98,2**.

Klasa: 954-01/23-01/01
Urbroj: 555-01-05-03-23-10
Zagreb, 8. svibnja 2023.

Glavna ravnateljica
Lidija Brković, v. r.

881

Državni zavod za statistiku objavljuje

INDEKS

POTROŠAČKIH CIJENA U TRAVNJU 2023.

Indeks potrošačkih cijena u travnju 2023. u odnosu na ožujak 2023. iznosi **101,0**.

Klasa: 956-03/23-01/3
Urbroj: 555-01-04-06-01-23-08
Zagreb, 16. svibnja 2023.

Glavna ravnateljica
Lidija Brković, v. r.

HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

882

Na temelju članka 12. stavka 2. točke 2., članka 16. stavka 1. točke 1. i članka 41. stavka 6. Zakona o elektroničkim komunikacijama (»Narodne novine« br. 76/2022), Vijeće Hrvatske regulatorne agencije za mrežne djelatnosti na sjednici održanoj 11. svibnja 2023. godine donosi

PRAVILNIK

O NAČINU I ROKOVIMA PROVEDBE MJERA ZAŠTITE SIGURNOSTI MREŽA I USLUGA

I. OPĆE ODREDBE

Sadržaj pravilnika

Članak 1.

Ovim Pravilnikom propisuju se način i rokovi u kojima operatori javnih elektroničkih komunikacijskih mreža i usluga te mreža koje se upotrebljavaju kao potpora sustavima kritičnih infrastrukturu-

ra (dalje: operatori) moraju poduzeti odgovarajuće tehničke i ustrojstvene mjere kako bi se zaštitila sigurnost njihovih mreža i usluga, način i rokovi izvješćivanja Hrvatske regulatorne agencije za mrežne djelatnosti (dalje: Agencija) o sigurnosnim incidentima od značajnog utjecaja na rad mreža operatora ili obavljanje njihovih usluga, obveza provedbe godišnje revizije mjera sigurnosti mreža i usluga operatora te mjerila i način certificiranja pravnih osoba koje je za provedbu te revizije ovlastila Agencija.

Značenje pojmova

Članak 2.

U smislu ovog Pravilnika pojedini pojmovi imaju sljedeće značenje:

1. *ENISA (eng. European Union Agency for Cybersecurity)*: Europska agencija za kibernetičku sigurnost

2. *IKT proizvod, proces ili usluga*: značenje kako je propisano člankom 2. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013

3. *Nacionalna taksonomija računalno-sigurnosnih incidenata*: ujednačeni kriteriji pri klasifikaciji računalno-sigurnosnih incidenata na nacionalnoj razini u vlastitim informacijskim sustavima i računalnim mrežama

4. *Nacionalni CERT*: nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj

5. *Nacionalno akreditacijsko tijelo*: značenje kako je propisano člankom 2. točkom 11. Uredbe (EZ) br. 765/20085 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93

6. *PiXi platforma*: nacionalna platforma za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim prijetnjama i incidentima te prijavu značajnih računalno-sigurnosnih incidenata

7. *politika informacijske sigurnosti*: skup pravila i postupaka koji definiraju na koji način se sredstva i resursi informacijske tehnologije trebaju koristiti i štiti te kako njima upravljati

8. *računalno-sigurnosni incident*: sigurnosni incident sukladno kriterijima Nacionalne taksonomije računalno-sigurnosnih incidenata

9. *sigurnosni incident*: događaj koji ima stvarni negativni učinak na sigurnost elektroničkih komunikacijskih mreža ili usluga

10. *sigurnost mreža i usluga*: sposobnost elektroničkih komunikacijskih mreža i usluga da određenom pouzdanosti odolijevaju bilo kojoj radnji kojom se ugrožava dostupnost, autentičnost, cjelovitost ili povjerljivost tih mreža i usluga, pohranjenih, prenesenih ili obrađenih podataka, ili povezanih usluga koje se pružaju ili su dostupne tim elektroničkim komunikacijskim mrežama ili uslugama

11. *utjecaj na autentičnost*: utjecaj na svojstvo da je entitet ono za što tvrdi da jest (npr. kompromitiranje korisničkog identiteta)

12. *utjecaj na cjelovitost*: utjecaj na svojstvo točnosti i potpunosti (npr. namjerno ili slučajno neovlašteno mijenjanje ili uništavanje komunikacijskih podataka ili metapodataka),

13. *utjecaj na dostupnost*: djelovanje na kontinuitet pružanja usluge, degradiranje performanse usluge, te djelomični ili potpuni pad mreže ili usluge

14. *utjecaj na povjerljivost*: dostupnost informacije neovlaštenim osobama, pojedincima, entitetima ili procesima (npr. kompromitiranje povjerljivosti komunikacije, komunikacijskih podataka ili metapodataka)

15. *značajan računalno-sigurnosni incident*: računalno-sigurnosni incident koji utječe na kritične podatke (neklasificirane i klasificirane) i/ili informacijske sustave i računalne mreže u javnom i privatnom sektoru, posebice na sustave koji su dio nacionalne kritične infrastrukture, na kojima se ti podaci obrađuju i kojima se prenose te koji može ostvariti i/ili ostvaruje negativan utjecaj na svakodnevni život velikog broja građana, nacionalnu ekonomiju i nacionalnu sigurnost u cjelini.

II. MJERE ZA ZAŠTITU SIGURNOSTI MREŽA I USLUGA

Opće obveze

Članak 3.

(1) Operatori su obvezni poduzeti odgovarajuće tehničke i ustrojstvene mjere, uključujući kodiranje (enkripciju) kada je to primjereno, radi zaštite sigurnosti svojih mreža i usluga te sprječavanja i umanjenja utjecaja sigurnosnih incidenata na korisnike i na druge elektroničke komunikacijske mreže i usluge, pri čemu poduzete mjere moraju osigurati razinu sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže i usluga, vodeći računa o raspoloživim tehničkim i tehnološkim rješenjima.

(2) Tehničke i ustrojstvene mjere iz stavka 1. ovog članka minimalno uključuju:

- sustav upravljanja rizicima
- sigurnosne zahtjeve za osoblje
- sigurnost sustava i prostora
- upravljanje postupcima
- upravljanje sigurnosnim incidentima
- upravljanje kontinuitetom poslovanja
- nadzor i testiranje sigurnosti
- svjesnost o sigurnosnim prijetnjama.

(3) Pri poduzimanju mjera iz stavka 1. i 2. ovog članka, operatori u najvećoj mogućoj mjeri primjenjuju mjerodavne tehničke smjernice ENISA-e o sigurnosnim mjerama, prijetnjama te druge relevantne smjernice.

(4) Popis referentnih normi za provođenje mjera iz stavka 1. i 2. ovog članka nalazi se u Dodatku 1. ovog Pravilnika.

(5) Mjerama iz stavka 2. ovog članka mora se osigurati i primjena sigurnosne politike kod obrade i zaštite osobnih podataka.

(6) Operatori su obvezni dokumentirati poduzete i implementirane mjere iz stavka 2. ovog članka te ih učiniti dostupnim Agenciji na njezin zahtjev. Agencija nadzire mjere koje u provedbi ovog članka poduzimaju operatori te može predlagati zaštitne mjere u skladu s odgovarajućom razinom sigurnosti.

(7) Operatori koji imaju više od 100 000 korisnika obvezni su elektroničkim putem jednom godišnje, najkasnije do kraja mjeseca siječnja, dostaviti Agenciji politiku informacijske sigurnosti za prethodnu godinu, a na zahtjev Agencije i više puta tijekom godine. Operatori koji imaju manje od 100 000 korisnika moraju dostaviti Agenciji politiku informacijske sigurnosti na njezin zahtjev.

Sigurnost 5G mreža i usluga

Članak 4.

(1) U odnosu na 5G mreže, politika informacijske sigurnosti mora sadržavati i popis kritičnih mrežnih komponenti i osjetljivih dijelova 5G mreže, uzimajući u obzir popis kritičnih i osjetljivih dijelova 5G mreže definiran dokumentom EU koordinirana procjena rizika kibernetičke sigurnosti u 5G mrežama.

(2) Uz mjere iz članka 3. stavka 2. ovoga Pravilnika, operatori za 5G moraju implementirati sljedeće dodatne tehničke i organizacijske mjere:

- oprema za kritične i osjetljive dijelove 5G mreže mora zadovoljavati mjerodavne 5G standarde, osobito 3GPP standarde sukladno mjerodavnim smjernicama ENISA-e, kao i primjenjive EU i nacionalne programe (certifikacijske sheme) kibernetičke sigurnosti

- sustav sigurnosti opskrbe 5G opreme, što između ostalog uključuje procjenu sigurnosti svih odabranih izvođača, proizvođača i njihovih dobavljača, te sustav nadzora nad načinom i kvalitetom pružanja ugovoreni poslova i usluga uz odgovarajuću primjenu mjerodavnih smjernica ENISA-e vezano uz nabavu sigurnih IKT procesa, proizvoda i usluga

- korištenje dobavljača koji dokažu odgovarajuću razinu dugoročne održivosti/otpornosti opreme i/ili IKT procesa, proizvoda i usluga

- provođenje sigurnosne kontrole u skladu s mjerodavnim standardima za sigurnost 5G mreža i usluga

- sustav ograničenja i nadzora udaljenog pristupa kritičnom dijelu mreže i informacijskom sustavu od trećih strana te implementacija, gdje je moguće, principa najmanje privilegiranog i podjela dužnosti

- operativni centar (NOC) i sigurnosno-operativni centar (SOC) mora se nalaziti na području neke od zemalja članicama Europske unije

- NOC i SOC, svako u svom djelokrugu rada, moraju provoditi nadzor kritičnih mrežnih komponenti i osjetljivih dijelova 5G mreža u svrhu pravovremenog otkrivanja nepravilnosti te prepoznavanja i sprečavanja prijetnji

- mjere zaštite upravljanja prometom komunikacijskih mreža ili usluga kako bi se spriječile neovlaštene promjene na mrežnim ili uslužnim komponentama

- mjere fizičke zaštite MEC-a (Multi-access Edge Computing) i baznih stanica temeljeno na procjeni rizika primjerice s obzirom na to gdje se komponente raspoređuju i koriste, te posebne mjere pristupa ograničenom broju sigurnosno provjerenom, kvalificiranom osoblju uz ograničen i nadziran pristup trećih strana

- alati i procesi za osiguravanje integriteta softvera prilikom njegovog ažuriranja i primjene sigurnosnih zakrpa, pouzdane identifikacije i praćenja promjena i statusa zakrpa, osobito u virtualiziranim mrežnim funkcijama

- procedure u svrhu oporavka u slučaju incidenata koji ima utjecaj i na međuovisne kritične sektore i usluge.

(3) Pri poduzimanju mjera iz stavka 2. ovog članka, operatori u najvećoj mogućoj mjeri primjenjuju mjerodavne tehničke smjernice ENISA-e o sigurnosnim mjerama 5G mreža.

(4) Operatori su obvezni dokumentirati mjere iz stavka 2. ovog članka.

Revizija sigurnosti mreža i usluga

Članak 5.

(1) Operatori su obvezni najmanje jednom godišnje provoditi procjenu rizika te reviziju sigurnosti mreža i usluga kako bi se utvrdilo jesu li ispunjene minimalne mjere sigurnosti iz Dodatka 1 i članka 4. ovog Pravilnika, uzimajući pri tom u obzir rezultate prethodnih revizija.

(2) Reviziju obavlja vanjsko revizorsko tijelo koje je Agencija za to ovlastila sukladno članku 9. ovoga Pravilnika.

(3) Procjenu rizika te nalaz revizije iz stavka 1. ovog članka, zajedno s planom tretiranja rizika te planom uklanjanja uočenih nedostataka, operatori koji imaju više od 100 000 korisnika obvezni su dostaviti Agenciji do 30. svibnja tekuće godine za prethodnu godinu. Operatori koji imaju manje od 100 000 korisnika obvezni su dostaviti Agenciji nalaz revizije na njezin zahtjev.

(4) U slučaju da plan uklanjanja uočenih nedostataka iz stavka 3. ovog članka ne ocijeni primjerenim za sprječavanje i umanjenje utjecaja sigurnosnih i računalno-sigurnosnih incidenata na korisnike usluga i/ili za osiguranje sigurnosti mreža i usluga, Agencija može operatorima odrediti dodatne mjere.

(5) Agencija može donositi obvezujuće upute, što uključuje mogućnost naloga operatorima za poduzimanjem mjera u svrhu sprečavanja sigurnosnih incidenata kada se utvrdi znatna prijetnja te mjera za uklanjanje posljedica sigurnosnih incidenata kao i rokove provedbe tih mjera.

III. SIGURNOSNI INCIDENTI

Obavješćavanje Agencije o sigurnosnim incidentima

Članak 6.

(1) Operatori su obvezni obavijestiti Agenciju o sigurnosnom incidentu koji je značajnije utjecao na rad mreža ili obavljanje usluga sukladno kriterijima za izvješćivanje iz Dodatka 2., pri čemu operatori provjeravaju ispunjavanje Kvantitativnih kriterija te ukoliko isti nisu zadovoljeni provjeravaju ispunjenost Kvalitativnih kriterija iz navedenog Dodatka.

(2) U slučaju da dođe do ispada barem jednog od dva redundantna kabela/informacijska sustava, operatori su obvezni prijaviti navedeni sigurnosni incident kao incident koji ima utjecaj na redundanciju, odgovarajućom primjenom predloška iz Dodatka 3. ovog Pravilnika.

(3) Obavijest o sigurnosnim incidentima iz stavka 1. ovog članka mora se dostaviti Agenciji bez odgode, čim su podaci dostupni, i to putem predloška propisanog u Dodatku 3. ovog Pravilnika:

1. u roku od najviše 1 sat nakon ispunjavanja kriterija za izvješćivanje, odnosno isteka minimalnog trajanja sigurnosnog incidenta iz Dodatka 2,

2. u roku od najviše 1 sat nakon otklanjanja sigurnosnog incidenta,

3. u roku od najviše 20 dana od dana otklanjanja sigurnosnog incidenta.

(4) U slučaju nastanka sigurnosnog incidenta koji ispunjava kvantitativne ili kvalitativne kriterije za izvješćivanje iz Dodatka 2. te je ujedno došlo do značajnog računalno-sigurnosnog incidenta sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata, operatori su obavezni dostaviti Agenciji obavijest o navedenom incidentu putem predloška iz Dodatka 3. ovog Pravilnika i Nacionalnom CERT-u putem PiXi platforme. Dodatne obveze za prijavu značajnih računalno-sigurnosnih incidenata propisane su u članku 7. ovog Pravilnika.

(5) Operatori su obvezni osigurati Agenciji podatke za kontakt sukladno Dodatku 3 ovog Pravilnika u svrhu brze razmjene informacija o sigurnosnim incidentima, te pružiti potrebne tehničke informacije Agenciji radi praćenja sigurnosti njihovih mreža i usluga.

(6) Sve obavijesti o sigurnosnim incidentima moraju se dostavljati Agenciji elektroničkim putem, zaštićeno zaporkom, na adresu elektroničke pošte incidenti@hakom.hr ili na drugi prikladan način sukladno predlošku iz Dodatka 3. ovog Pravilnika. Nakon što operator prvi puta dostavi obavijest o sigurnosnom incidentu, Agencija će operatoru dostaviti daljnje upute, odnosno upute vezane uz dostavu zaporka.

(7) Agencija može zatražiti dopunu obavijesti iz stavka 3. u svrhu praćenja određenog sigurnosnog incidenta te boljeg razumijevanja prirode nastalog sigurnosnog incidenta.

(8) Operatori mogu obavijestiti Agenciju i o drugim, po njihovom mišljenju, važnim sigurnosnim incidentima koji se odnose na sigurnost mreža ili usluga, a koji nisu obuhvaćeni sigurnosnim incidentima iz stavka 1. ovog članka.

Dodatne obveze za značajne računalno-sigurnosne incidente

Članak 7.

(1) U slučaju svakog sigurnosnog incidenta, operatori uvijek moraju provjeriti je li došlo do značajnog računalno-sigurnosnog incidenta sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata.

(2) Obavijesti o značajnim računalno-sigurnosnim incidentima sukladno Nacionalnoj taksonomiji računalno-sigurnosnih incidenata moraju se dostavljati putem PiXi platforme u roku 72 sata od njihovog otkrivanja. Uvjeti i način korištenja ove platforme propisani su u Uvjetima korištenja PiXi platforme koja se nalazi na internet-skoj stranici Nacionalnog CERT-a.

(3) Nakon razmatranja prijavljenih incidenata, Agencija će u suradnji s Nacionalnim CERT-om, naložiti eventualnu dopunu izvješća te poduzimanje drugih mjera za sprečavanje ili uklanjanje incidenata, uključujući i davanje određenih preporuka, smjernica i upozorenja o sigurnosnim ugrozama.

(4) U slučaju potrebe pokretanja odgovarajućeg postupka iz nadležnosti Agencije u odnosu na prijavljene incidente, Agencija će aktivno surađivati s Nacionalnim CERT-om, te u slučaju potrebe zatražiti stručnu pomoć i koordinaciju pri definiranju konkretnih aktivnosti i korektivnih mjera u vezi s nastalim ili potencijalnim računalno-sigurnosnim incidentima.

Obavješćavanje drugih subjekata o sigurnosnim incidentima

Članak 8.

(1) Operatori su obvezni bez odgode:

1. na jasan i lako dokaziv način obavijestiti korisnike svojih usluga o sigurnosnom incidentu koji je značajnije utjecao na rad mreža ili obavljanje njihovih usluga, sukladno kriterijima za izvješćivanje iz Dodatka 2. te objaviti informacije o nastalom značajnom incidentu na svojoj službenoj internetskoj stranici. Informacije o značajnom incidentu moraju sadržavati opis područja obuhvaćenog incidentom, koji može biti prikazan i u kartografskom obliku.

2. u slučaju posebne i znatne prijetnje od sigurnosnog incidenta u javnim elektroničkim komunikacijskim mrežama ili uslugama, obavijestiti korisnike svojih usluga na koje bi takva prijetnja mogla utjecati o svim mogućim mjerama zaštite ili pravnim sredstvima koja mogu uporabiti.

(2) Operatori će o vlastitom trošku poduzeti odgovarajuće i hitne mjere u svrhu sprječavanja nastanka štete u slučaju sigurnosnog incidenta.

IV. OVLAŠTENJE ZA OBAVLJANJE REVIZIJE SIGURNOSTI MREŽA I USLUGA

Ovlašteno revizorsko tijelo

Članak 9.

(1) Poslove revizije sigurnosti mreža i usluga operatora mogu obavljati pravne osobe na temelju rješenja o ovlaštenju koje donosi Agencija.

(2) Agencija će izdati ovlaštenje ako je pravna osoba akreditirana od strane Hrvatske akreditacijske agencije ili drugog nacionalnog akreditacijskog tijela u smislu Uredbe (EZ) br. 765/2008, za obavljanje revizije informacijskih sustava sukladno važećim standardima ISO 27 001 i ISO 22 301.

(3) Agencija donosi rješenje o ovlaštenju iz stavka 1. ovog članka temeljem zahtjeva pravne osobe. Zahtjev koji pravna osoba podnosi Agenciji mora sadržavati sljedeće:

- podatke o podnositelju zahtjeva
- presliku potvrde o akreditaciji iz stavka 2. ovoga članka.

(4) Rješenje o ovlaštenju iz stavka 1. ovog članka izdaje se pravnim osobama s rokom valjanosti određenim akreditacijom iz stavka 2. ovog članka.

(5) Agencija će ukinuti rješenje o ovlaštenju iz stavka 1. ovog članka ako pravna osoba više ne ispunjava uvjete iz stavka 2. ovog članka.

(6) Popis ovlaštenih pravnih osoba za obavljanje revizije sigurnosti mreža i usluga operatora vodi Agencija, koja ga redovito dopunjuje i objavljuje na svojim internetskim stranicama.

V. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 10.

Operatori mreža koje se upotrebljavaju kao potpora sustavima kritičnih infrastruktura obvezni su uskladiti svoj rad i poslovanje s odredbama ovog Pravilnika u roku od godine dana od dana stupanja na snagu ovog Pravilnika.

Članak 11.

Stupanjem na snagu ovog Pravilnika prestaje vrijediti Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (»Narodne novine« br. 112/21).

Članak 12.

Ovaj Pravilnik stupa na snagu osmoga dana od dana objave u »Narodnim novinama«.

Klasa: 011-02/23-02/05

Urbroj: 376-05-4-23-1

Zagreb, 11. svibnja 2023.

Predsjednik Vijeća
Tonko Obuljen, v. r.

DODATAK 1

MINIMALNE MJERE SIGURNOSTI

Minimalne mjere sigurnosti	Referentne norme
Sustav za upravljanja rizicima	ISO 27001
	ISO 27002
	ISO 27005
	ISO 27036-3
Sigurnosni zahtjevi za osoblje	ISO 27001
	ISO 27002
Sigurnost sustava i objekata (prostora)	ISO 27001
	ISO 27002
Upravljanje operacijama (postupcima)	ISO 27001
	ISO 27002
Upravljanje sigurnosnim incidentima	ISO 27001
	ISO 27002
Upravljanje kontinuitetom poslovanja	ISO 27001
	ISO 27002
	ISO 22301

Nadzor i testiranje sigurnosti	ISO 27001 ISO 27002
Svjesnost o sigurnosnim prijetnjama	ISO 27001 ISO 27002

DODATAK 2

KVANTITATIVNI KRITERIJI ZA IZVJEŠČIVANJE

Dostupnost:	Minimum krajnjih korisnika obuhvaćenih sigurnosnim incidentom	Minimalno trajanje sigurnosnog incidenta
Govorne usluge u nepokretnoj mreži	12 000	8 sati
Govorne usluge u nepokretnoj mreži	24 000	6 sati
Govorne usluge u nepokretnoj mreži	60 000	4 sata
Govorne usluge u nepokretnoj mreži	120 000	2 sata
Govorne usluge u nepokretnoj mreži	180 000	1 sat
Govorne usluge u pokretnoj mreži	45 000	8 sati
Govorne usluge u pokretnoj mreži	90 000	6 sati
Govorne usluge u pokretnoj mreži	225 000	4 sata
Govorne usluge u pokretnoj mreži	450 000	2 sata
Govorne usluge u pokretnoj mreži	675 000	1 sat
Usluge pristupa internetu u nepokretnoj mreži	11 000	8 sati
Usluge pristupa internetu u nepokretnoj mreži	22 000	6 sati
Usluge pristupa internetu u nepokretnoj mreži	55 000	4 sata
Usluge pristupa internetu u nepokretnoj mreži	110 000	2 sata
Usluge pristupa internetu u nepokretnoj mreži	165 000	1 sat
Usluge pristupa internetu u pokretnoj mreži	50 000	8 sati
Usluge pristupa internetu u pokretnoj mreži	100 000	6 sati
Usluge pristupa internetu u pokretnoj mreži	250 000	4 sata
Usluge pristupa internetu u pokretnoj mreži	500 000	2 sata
Usluge pristupa internetu u pokretnoj mreži	750 000	1 sat
Brojevno neovisne interpersonalne komunikacijske usluge	50 000	8 sati
Brojevno neovisne interpersonalne komunikacijske usluge	100 000	6 sati
Brojevno neovisne interpersonalne komunikacijske usluge	250 000	4 sata
Brojevno neovisne interpersonalne komunikacijske usluge	500 000	2 sata
Brojevno neovisne interpersonalne komunikacijske usluge	750 000	1 sat
Povjerljivost/autentičnost/cjelovitost	Minimum krajnjih korisnika obuhvaćenih sigurnosnim incidentom	Minimalno trajanje sigurnosnog incidenta
Govorna usluga u nepokretnoj mreži	12 000	Neovisno o trajanju
Govorna usluga u pokretnoj mreži	45 000	Neovisno o trajanju

Usluga pristupa internetu u nepokretnoj mreži	11 000	Neovisno o trajanju
Usluga pristupa internetu u pokretnoj mreži	50 000	Neovisno o trajanju
Brojevno neovisna interpersonalna komunikacijska usluga	50 000	Neovisno o trajanju

KVALITATIVNI KRITERIJI ZA IZVJEŠČIVANJE

Sigurnosni incident se odnosi na: govornu uslugu u nepokretnoj mreži / govornu uslugu u pokretnoj mreži / uslugu pristupa internetu u nepokretnoj mreži / uslugu pristupa internetu u pokretnoj mreži / brojevno neovisnu interpersonalnu komunikacijsku uslugu / uslugu komunikacije između strojeva (M2M) / uslugu odašiljanja radijskih i televizijskih programa	Dostupnost/povjerljivost/autentičnost/cjelovitost usluge
1. Značajan zbog geografskog obuhvata incidenta (prekogranično, nacionalno, velika udaljena/ruralna područja, otoci, grad Zagreb i sl.) 2. Značajan zbog utjecaja na gospodarstvo i društvo ili na korisnike (nemogućnost pristupa 112, nacionalnim brojevima za hitne službe, utjecaj na javne sustave upozorenja, velika materijalna šteta, visoki rizici za javnu sigurnost ili gubitak života, medijska pokrivenost, utjecaj na kontinuitet osnovnih usluga ili kritičnih sektora/operatora, utjecaj na posebne dane kao dana izbora ili referenduma.)	neovisno o trajanju i broju korisnika

DODATAK 3

PREDLOŽAK ZA IZVJEŠČIVANJE O SIGURNOSNOM INCIDENTU

Potrebni podaci	Popunjiva operator		
Naziv operatora			
Datum podnošenja izvještaja			
Datum i vrijeme nastanka/otkrivanja sigurnosnog incidenta		Datum i vrijeme otklanjanja sigurnosnog incidenta	
Opis incidenta			
Tip incidenta	<input type="checkbox"/> A – Ispad usluge (npr. kontinuitet, dostupnost) <input type="checkbox"/> D – Prijetnja ili ranjivost (npr. otkrivanje slabosti u kriptiranju) <input type="checkbox"/> B – Drugi utjecaj na usluge (npr. povjerljivost, cjelovitost, autentičnost) <input type="checkbox"/> E – Utjecaj na redundanciju (npr. prelazak na redundanciju ili sigurnosni sustav) <input type="checkbox"/> C – Utjecaj na druge sustave (npr. ucjenjivački zlonamjerni softver u uredskoj mreži, bez utjecaja na uslugu) <input type="checkbox"/> F – Zamalo incident (npr. aktivacija sigurnosnih mjera)		
Obuhvaćene usluge	<input type="checkbox"/> Nepokretna telefonija <input type="text"/> Broj korisnika <input type="text"/> Trajanje <input type="checkbox"/> Pokretna telefonija <input type="text"/> Broj korisnika <input type="text"/> Trajanje <input type="checkbox"/> Nepokretni internet <input type="text"/> Broj korisnika <input type="text"/> Trajanje <input type="checkbox"/> Pokretni internet <input type="text"/> Broj korisnika <input type="text"/> Trajanje <input type="checkbox"/> OTT usluge <input type="text"/> Broj korisnika <input type="text"/> Trajanje <input type="checkbox"/> M2M <input type="text"/> Broj korisnika <input type="text"/> Trajanje <input type="checkbox"/> Emitiranje <input type="text"/> Broj korisnika <input type="text"/> Trajanje <input type="checkbox"/> Drugo <input type="text"/> Broj korisnika <input type="text"/> Trajanje		

Izvorni uzrok	<input type="checkbox"/> Sistemske greške <input type="checkbox"/> Ljudske greške <input type="checkbox"/> Zlonamjerne radnje <input type="checkbox"/> Prirodni fenomen <input type="checkbox"/> Greška treće strane
Tehnologija usluga ili podusluga	<input type="checkbox"/> Kabelska <input type="checkbox"/> DSL <input type="checkbox"/> Email <input type="checkbox"/> Optika <input type="checkbox"/> GRPS/EDGE <input type="checkbox"/> GSM <input type="checkbox"/> Instant messaging protokol <input type="checkbox"/> LTE <input type="checkbox"/> MTC <input type="checkbox"/> PSTN <input type="checkbox"/> Signalizacijski protokol <input type="checkbox"/> UMTS <input type="checkbox"/> URLLC <input type="checkbox"/> VoIP <input type="checkbox"/> Web/App <input type="checkbox"/> eMBB <input type="checkbox"/> Drugo
Tehnički uzroci	<input type="checkbox"/> Palež <input type="checkbox"/> Presjek kabela <input type="checkbox"/> Krađa kabela <input type="checkbox"/> Prekid hlađenja <input type="checkbox"/> DDoS napad <input type="checkbox"/> Zemljotres <input type="checkbox"/> Prisluškiavanje <input type="checkbox"/> Elektromagnetska interferencija <input type="checkbox"/> Vanjski okolišni uzroci <input type="checkbox"/> Neispravna promjena/ažuriranje hardvera <input type="checkbox"/> Neispravna promjena/ažuriranje softvera <input type="checkbox"/> Vatra <input type="checkbox"/> Poplava <input type="checkbox"/> Iscrpljene zalihe goriva <input type="checkbox"/> Kvar na hardveru <input type="checkbox"/> Krađa hardvera <input type="checkbox"/> Obilan snijeg/led <input type="checkbox"/> Oluja <input type="checkbox"/> Krađa identiteta <input type="checkbox"/> Zlonamjerni softveri i virusi <input type="checkbox"/> Preotimanje mrežnog prometa <input type="checkbox"/> Preopterećenje <input type="checkbox"/> Phishing <input type="checkbox"/> Proceduralna mana <input type="checkbox"/> Prekid napajanja <input type="checkbox"/> Strujni udari <input type="checkbox"/> Sigurnosno isključivanje <input type="checkbox"/> Softverska greška <input type="checkbox"/> Iskorištavanje ranjivosti <input type="checkbox"/> Požar <input type="checkbox"/> Drugo

Tehnička imovina obuhvaćena incidentom	<input type="checkbox"/> Adresni poslužitelji <input type="checkbox"/> App <input type="checkbox"/> Rezervno napajanje <input type="checkbox"/> Sustav naplate i posredovanja <input type="checkbox"/> Zgrade i fizički sigurnosni sustavi <input type="checkbox"/> Pohrana u oblaku <input type="checkbox"/> Sustav hlađenja <input type="checkbox"/> Inteligentni mrežni uređaji <input type="checkbox"/> Međukonekcijske točke <input type="checkbox"/> Logički sigurnosni sustavi <input type="checkbox"/> Bazine stanice i upravljački sklopovi <input type="checkbox"/> Centar za razmjenu poruka <input type="checkbox"/> Mobilni prospojnici <input type="checkbox"/> Registar mobilnih korisnika i lokacija <input type="checkbox"/> Operativni sustav potpore <input type="checkbox"/> Nadzemni kablovi <input type="checkbox"/> PSTN prospojnici <input type="checkbox"/> Sustav napajanja sustavi <input type="checkbox"/> SIM/eSIM <input type="checkbox"/> Ulični kabineti <input type="checkbox"/> Podmorski kablovi <input type="checkbox"/> Pretplatnička oprema <input type="checkbox"/> Prospojnici i usmjerivači <input type="checkbox"/> Prijenosni čvorovi <input type="checkbox"/> Podzemni kablovi <input type="checkbox"/> Mrežna stanica <input type="checkbox"/> Drugo
Čimbenici značajnosti	<input type="checkbox"/> Broj obuhvaćenih korisnika <input type="checkbox"/> Trajanje incidenta <input type="checkbox"/> Geografska proširenost <input type="checkbox"/> Opseg poremećaja u funkcioniranju <input type="checkbox"/> Utjecaj na ekonomiju i društvo
Skala utjecaja	<input type="checkbox"/> Bez utjecaja <input type="checkbox"/> Manji utjecaj <input type="checkbox"/> Veliki utjecaj <input type="checkbox"/> Vrlo veliki utjecaj
Čimbenici ozbiljnosti prijetnje (za tip D)	<input type="checkbox"/> Troškovi ublažavanja <input type="checkbox"/> Potencijalna šteta <input type="checkbox"/> Stopa širenja prijetnje <input type="checkbox"/> Vjerojatnost izlaganja <input type="checkbox"/> Kritičnost potencijalno pogodnih sustava <input type="checkbox"/> Nedostatak dobrih rješenja za ublažavanje prijetnje
Ozbiljnost prijetnje (za tip D)	<input type="checkbox"/> Mala <input type="checkbox"/> Srednja <input type="checkbox"/> Velika
Rješavanje sigurnosnog incidenta i opis poduzetih mjera	

Mjere poduzete nakon otklanjanja sigurnosnog incidenta	
Dugoročne mjere	
Kontakt-podaci za praćenje procesa	
Ostale važne informacije	

AGENCIJA ZA ELEKTRONIČKE MEDIJE

883

Vijeće za elektroničke medije, u sastavu Josip Popovac, predsjednik Vijeća, Robert Tomljenović, zamjenik predsjednika Vijeća te Damir Bučević, Katija Kušec, Anita Malenica, Davor Marić i Željko Topić, članovi Vijeća, na temelju odredbe članka 85. stavka 8. i 9. Zakona o elektroničkim medijima (»Narodne novine«, broj 111/21 i 114/22), nakon provedenog postupka nadmetanja sukladno Obavijesti o namjeri davanja koncesije za obavljanje djelatnosti pružanja medijske usluge digitalnog radija (DAB+) br. 01/23, klasa: UP/I-614-03/23-02/0001, urbroj: 114-06/04-23-01, »Narodne novine« broj 26/23 i utvrđivanja uvjeta za davanje koncesije, na 15-23. sjednici održanoj 4. svibnja 2023., donijelo je

ODLUKU

I. Nakon provedenog postupka nadmetanja sukladno Obavijesti o namjeri davanja koncesije za obavljanje djelatnosti pružanja medijske usluge digitalnog radija (DAB+) br. 01/23 za područje digitalne regije MUX 1 (Republika Hrvatska) objavljene na temelju Odluke Vijeća za elektroničke medije od 2. ožujka 2023., kao najpovoljniji ponuditelj za dva kanala odabrana su trgovačka društva EXTRA FM ZAGREB d.o.o., Avenija Većeslava Holjevca 29/I, Zagreb, OIB: 79875421716 i HAPPY FM d.o.o., Kolodvorska 29, Velika Gorica, OIB: 81362164358 te im se daje koncesija za obavljanje djelatnosti pružanja medijske usluge digitalnog radija na predmetnom području.

II. Vrijeme trajanja koncesije je 20 (dvadeset) godina.

III. Visina godišnje naknade za koncesiju sastoji se od fiksnog i varijabilnog dijela. Fiksni dio godišnje naknade za koncesiju plaća se na svakih 50.000 stanovnika u iznosu od 66,36 eura. Varijabilni dio godišnje naknade za koncesiju plaća se u iznosu od 0,15% od ukupnoga godišnjeg bruto prihoda koje je u prethodnoj godini ostvario ponuditelj. Varijabilni dio godišnje naknade za koncesiju ponuditelj plaća na iznos ostvarenog ukupnog godišnjeg bruto prihoda od obavljanja djelatnosti pružanja medijskih usluga televiziji i radija iznad 663.614,04 eura. Minimalni iznos godišnje naknade za koncesiju iznosi 66,36 eura.

IV. Odabrani ponuditelji obvezni su roku od 90 (devedeset) dana od dana objave ove Odluke u »Narodnim novinama« uputiti Hrvatskoj regulatornoj agenciji za mrežne djelatnosti (HAKOM) zahtjev za obavljanje tehničkog pregleda radi utvrđivanja prostornih i tehničkih uvjeta. Ako odabrani ponuditelji u tom roku ne podnesu zahtjev Hrvatskoj regulatornoj agenciji za mrežne djelatnosti, smatrat će se da su odustali od koncesije.

V. Sukladno članku 21. stavku 5. Pravilnika o sadržaju i postupku raspisivanja obavijesti o namjeri davanja koncesija za obavljanje