PRAVILNIK

O INFORMACIJSKOJ SIGURNOSTI

Općina Topusko

Topusko, 26. rujna 2019.

SADRŽAJ

U skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i Zakonom o provedbi Opće uredbe o zaštiti podataka („Narodne novine“ broj 42/18.), općinski načelnik Općine Topusko, 26. rujna 2019. godine, donio je

PRAVILNIK O INFORMACIJSKOJ SIGURNOSTI

1 Uvod

Članak 1.

Ovaj Pravilnik donesen je sa svrhom da:

- Definira prihvatljive načine ponašanja u svezi korištenja računalnog informacijskog sustava Općine Topusko (u daljnjem tekstu: Općina).
- Raspodjeli zadatke i odgovornosti nadležnih osoba.
- Zaštiti investiciju Općine u računalni informacijski sustav.
- Zaštiti informacije i podatke koji se u sustavu kreiraju, prenose, pohranjuju i obrađuju.
- Propiše sankcije u slučaju nepridržavanja odredbi ovog pravilnika.

Sastavni dio ovog Pravilnika su i procedure:

- Procedura upravljanja zaporkama,
- Procedura upravljanja zaštitom od zlonamjernog softvera

U Pravilniku se koriste i pojmovi iz Uredbe (EU) 2016/679. Prema toj Uredbi Općina je Voditelj obrade a autori programskih rješenja koje Općina koristi su Izvršitelji obrade.

2 Opseg primjene Pravilnika

Članak 2.

Ovaj Pravilnik odnosi se na zaposlenike i vanjske suradnike (u daljnjem tekstu termin korisnik odnosit će se na ove osobe koje koriste informatički sustav Općine) kojima se dopušta uporaba računalnog informacijskog sustava Općine.

Pravilnik obuhvaća računalni informacijski sustav Općine i sve sadržaje koji se prenose, pohranjuju i obrađuju u tom sustavu, sadržaje pohranjene na svim osobnim računalima u vlasništvu Općine, kao i sve poslužitelje koji su u administrativnoj domeni ili vlasništvu Općine.

3 Odgovornost

Članak 3.

Za primjenu ovog Pravilnika i korištenje informatičke opreme u vlasništvu Općine najodgovornija je osoba određena posebnom odlukom načelnika Općine (u daljnjem tekstu Referent za IT sigurnost).

Referent za IT sigurnost je odgovoran za:

- administriranje i održavanje sigurnosti računalnog informacijskog sustava što uključuje materiju koju uređuje ovaj Pravilnik i sve pridružene procedure,
- razvijanje i održavanje pisanih standarda i procedura kojima se osigurava primjena i pridržavanje odredbi ovog Pravilnika i procedura,
- pružanje odgovarajuće podrške korisnicima u ispunjavanju njihove obveze u odnosu na ovaj Pravilnik i pripadajuće procedure.

Svi korisnici obvezni su proučiti i primjenjivati ovaj Pravilnik kao i njemu pridružene procedure.

Članak 4.

Općina štiti svoju računalnu opremu, sklopovlje, programsku podršku, podatke i dokumentaciju od zlouporabe, krađe, neovlaštene uporabe i upliva okoliša.

Za sigurnost računalnog informacijskog sustava Općine odgovorni su korisnici i Referent za IT sigurnost, svaki u svom dijelu odgovornosti propisane ovim Pravilnikom.

Povjerljivost i integritet podataka pohranjenih na računalnom informacijskom sustavu Općine moraju biti zaštićeni sustavom kontrole pristupa kako bi se osiguralo da samo ovlašteni korisnici imaju pristup potrebnim informacijama. Taj pristup treba biti ograničen na samo one informacijske sustave i mogućnosti koje su korisniku nužne za njegove poslovne aktivnosti.

Članak 5.

Referent za IT sigurnost je odgovoran za sve instalacije, odspajanja, promjene i premještanje računalne opreme. Korisnici ne smiju samostalno poduzimati takve radnje (ovo se ne odnosi na prijenosna računala).

Članak 6.

Korisnici, glede informacijske sigurnosti, su obvezni pridržavati se slijedećih uputa:

- Mediji s podacima i programskom podrškom (CD-ovi, DVD-ovi, diskovi, USB stick-ovi i ostali mediji) za vrijeme kada nisu u upotrebi, ne smiju biti izloženi na lako dostupnim mjestima neovlaštenim osobama;
- Mediji koji sadrže povjerljive i važne podatke trebaju biti čuvani u adekvatnim zaključanim kasama ili metalnim ormarima;
- Podatkovni mediji trebaju se čuvati podalje od nepovoljnih utjecaja okoliša kao što su toplina, direktno sunčevo svjetlo, vlaga i elektromagnetska polja i slično;
- Utjecaji okoliša kao što su dim, hrana, tekućine, previsoka ili preniska vlažnost, previsoke ili preniske temperature moraju se izbjegavati;
- Prijenosna računala i drugu prijenosnu opremu koju rabi više korisnika, korisnici ne smiju iznositi izvan Općine bez odobrenja referenta za IT sigurnost;
- Korisnici se trebaju s pažnjom odnositi prema povjerenoj im računalnoj opremi;
- Korisnik će se smatrati odgovornim za štete nastale na računalnoj opremi ako su nastale uslijed nepažnje ili nepravilne uporabe

4 Administriranje korisnika

Članak 7.

Administriranje korisnika obuhvaća slijedeće aktivnosti:

- Otvaranje novog korisnika – dodjela korisničkog imena i zaporke – i dodjelu odgovarajućih prava u okviru svakog pojedinog softvera odnosno aplikacija koju korisnik ima pravo koristiti

Članak 8.

Za administriranje korisnika na nivou računalne mreže zadužen je referent za IT sigurnost.

Za administriranje korisnika na nivou aplikacije zadužen je administrator aplikacije.

Ako je administrator aplikacije vanjski suradnik (zaposlenik tvrtke čije se programsko rješenje koristi) zahtjev za administriranje korisnika dostavlja referent za IT sigurnost.

Nakon prestanka prava pristupa računalnom sustavu ili aplikaciji (prestanak službe, prestanak potrebe za korištenjem aplikacije) referent za IT sigurnost odnosno administrator aplikacije oduzima korisniku prava koja su mu bila dodijeljena.

5 Administriranje računalne opreme

Članak 9.

Računala i mrežna oprema moraju biti administrirani u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

Svako računalo mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju softvera.

Članak 10.

Računala se moraju konfigurirati na taj način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.

Članak 11.

Administratorska prava na računalima koja koriste više osoba može imati samo referent za IT sigurnost

Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa (npr. serveri, mrežna oprema i slično).

6 Zaporke i pristupni računi

Članak 12.

Zabranjuje se korištenje grupnih i univerzalnih pristupnih računa za pristup računalima i računalnim sustavima.

Svaka osoba obvezno mora pristupiti računalnom sustavu, računalima i informatičkim rješenjima (aplikacijama) Općine isključivo vlastitim pristupnim računom.

Članak 13.

Izuzetno, referent za IT sigurnost može na pismeno traženje načelnika Općine odobriti korisniku korištenje pristupnog računa druge osobe za pronalaženje i otklanjanje nepravilnosti rada sustava, o čemu treba sačiniti pisani dokument.

Nakon završetka radnji iz prethodnog stavka, obavezno treba promijeniti zaporku toga pristupnog računa.

Članak 14.

Korisnik:

- je odgovoran za sve računalne transakcije učinjene korištenjem dodijeljenog mu prijavnog imena i zaporke,
- ne smije njemu dodijeljene zaporke otkriti drugim osobama,
- treba odmah promijeniti svoju zaporku, ako posumnja da ju je netko drugi neovlašteno saznao,
- ne smije bilježiti zaporke na lako dostupnom mjestu,
- treba koristiti zaporke koje nije lako pogoditi,
- treba se odjaviti iz informacijskog sustava kada napušta radno mjesto.

Članak 15.

Referent za IT sigurnost obvezan je pohraniti sve administratorske zaporke u adekvatni metalni ormar (kasu) koju treba uvijek držati zaključanu.

Pohranjene zaporke trebaju biti svaka u zasebnoj zapečaćenoj kuverti, na kojoj treba pisati za koji je računalni sustav ili računalnu opremu, te datum kad je zadnji puta ažurirana.

Referent za IT sigurnost obvezan je redovito nakon svake promijene ažurirati pohranjene zaporke.

6.1 Rukovanje zaporkama

Članak 16.

Svi zaposlenici Općine koji u svome radu koriste računala dužni su pridržavati se ovih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Članak 17.

Kod otvaranja novog korisnika odvija se inicijalno postavljanje zaporke koja se, zajedno s korisničkim imenom, ispisuje na dokument koji se predaje korisniku.

Korisnik dobije dokument s inicijalnom zaporkom i popratnim tekstom u kojemu piše što su njegova prava i obaveze. Sadržaj i izgled dokumenta sastavni su Procedure upravljanja zaporkama.

Korisnik potpisom potvrđuje da je taj dokument primio.

Kod prvog prijavljivanja na sustav korisnik mora promijeniti inicijalnu zaporku i upisati novu zaporku, poznatu samo njemu, koju će koristiti u operativnom radu.

Članak 18.

U kreiranju zaporki svi korisnici su dužni poštivati slijedeća pravila:

- minimalna duljina zaporke je 6 znakova,
- zaporka mora biti kombinacija velikih i malih slova i znamenki,
- u zaporkama su dozvoljeni i znakovi interpunkcije,
- kao zaporku obavezno izbjegavati
    - korištenje riječi iz javno dostupnih rječnika,
    - korištenja imena bliskih osoba, ljubimaca, karakterističnih datuma i njihovih kombinacija,

7 Zaštita od zlonamjernog softvera

Članak 19.

Zaštita od zlonamjernog (*malware*) softvera (Računalni virusi, Računalni crvi, Trojanski konji, Logičke bombe, Rootkit, Spyware, Adware, Spamovi, Popupovi) je obavezna a provode ju:

- Davatelji informatičkih usluga na poslužiteljima elektroničke pošte
- Referent za IT sigurnost Općine na poslužiteljima Općine i osobnim računalima koja koriste zaposlenici Općine.

Članak 21.

Osobe koje provode zaštitu od zlonamjernog softvera nisu dužne čuvati elektronske poruke korisnika zaražene zlonamjernim softverom.

Osobe koje provode zaštitu od zlonamjernog softvera dužne su instalirati protuvirusne programe na sva korisnička računala i namjestiti ih tako da se izmjene u zaštiti automatski propagiraju s središnje instalacije ili s vanjskog poslužitelja, bez aktivnog sudjelovanja korisnika.

Članak 22.

Korisnici ne smiju samovoljno isključiti zaštitu od zlonamjernog softvera na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti program koji štiti od zlonamjernog softvera, korisnici moraju zatražiti dozvolu od referenta za IT sigurnost.

8 Fizička zaštita i sigurnost opreme

Članak 23.

U prostorijama Općine nalazi se informatička oprema (serveri, komunikacijska oprema, osobna računala) u vlasništvu Općine.

Referent za IT sigurnost (ili druga osoba po odluci načelnika) odgovorna je za održavanje ažurnog popis sve računalne opreme s popisom ugrađenih komponenti i inventarskim brojevima.

9 Neprekidnost poslovanja

Članak 24.

Kako bi se sačuvali podaci u slučaju nezgoda, kvarova na sklopovlju, požara ili ljudskih grešaka, neophodno je redovito izrađivati rezervne kopije svih podataka važnih za održavanje vitalnih funkcija informacijskog sustava i sklopovlja.

Članak 25.

Za izradu rezervnih kopija podataka zadužen je Izvršitelj obrade s kojim postoji odgovarajući ugovor o poslovno-tehničkoj suradnji.

Općina će osigurati da u ugovoru budu jasno definirane obaveze Izvršitelja obrade vezano uz izradu, pohranu i provjeru sigurnosnih kopija.

Članak 26.

Radi osiguranja neprekinutosti poslovanja, Općina će osigurati da u ugovoru o poslovno-tehničkoj suradnji, ili aneksu ugovora, budu jasno definirana pravila i obaveze Izvršitelja obrade za oporavak kritičnih sustava.

10 Licenčna prava

Članak 27.

Obveza je Općine i svih njegovih zaposlenika da poštuju zakone i propise o zaštiti intelektualnog vlasništva.

Općina je obvezno koristiti programsku podršku na temelju valjanih licenčnih prava.

Članak 28.

Općina programsku podršku i pripadajuću dokumentaciju koja nije u vlasništvu Općine nema pravo umnožavati i distribuirati bez dopuštenja proizvođača ili autora, osim za potrebe stvaranja sigurnosne kopije.

Članak 29.

Na računalima u vlasništvu Općine ne smije se, bez odobrenja općinskog načelnika, koristiti programska podrška nabavljena privatno.

11 Prekršaji i sankcije

Članak 30.

Nedozvoljenim se smatra svako korištenje računala i / ili računalnog programa na način koji bi doveo do povrede važećih zakona, propisa ili etičkih normi, a mogao bi izazvati materijalnu ili nematerijalnu štetu za Općinu.

Članak 31.

Lakšim oblicima nedozvoljenog korištenja računala i opreme smatra se:

- Ograničena uporaba nelicenciranog softvera,

- Skidanje (download) autorski zaštićenih datoteka bez plaćanja naknade ako su iste javno dostupne,
- Skidanje (download) i(ili) distribucija sadržaja neprimjerenog za poslovnu komunikaciju (pornografija i sl.),
- Slanje masovnih poruka, bile one komercijalne prirode ili ne, čime se nepotrebno troše mrežni resursi,
- Samovoljna instalacija softvera,
- Korištenje neprihvatljivih aplikacija i servisa zbog kojih se narušava sigurnost informacijskih sustava, nepotrebno troše mrežni resursi ili se nanosi bilo kakva materijalna i(ili) nematerijalna šteta Općini.

Članak 32.

Težim oblicima nedozvoljenog korištenja računala i opreme smatra se:

- Davanje podataka o vlastitom identitetu (korisničko ime, lozinka) drugima u Općini i / ili izvan Općine
- Preuzimanje tuđeg identiteta (korištenje opreme s tuđim korisničkim računom, slanje elektroničke pošte pod tuđim imenom, kupovanje preko interneta s tuđom kreditnom karticom itd.),
- Provaljivanje na druga računala,
- Traženje ranjivosti i sigurnosnih propusta. Korisnik ne smije samoinicijativno skenirati računala, probijati zaporke ili na bilo koji način istraživati sigurnosne propuste na računalima, bilo da ona pripadaju Općini ili ne,
- Napad uskraćivanjem resursa na druga računala,
- Vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti,
- Korištenje mrežnih resursa Općine na način priključivanja vlastitih – privatnih računala na računalnu mrežu Općine.

Članak 33.

Svi korisnici računalnog sustava Općine dužni su pridržavati se odredbi ovog Pravilnika kao i svih drugih internih dokumenata / odluka koje reguliraju korištenje računalnog sustava i informatičke opreme.

Kršenje odredbi ovog Pravilnika i pripadnih procedura može korisnika izložiti opozivu prava uporabe računalnog sustava Općine, te pokretanju stegovnog postupka sve do donošenja rješenja o prestanku službe iz razloga uvjetovanog iskrivljenim ponašanjem zaposlenika ili prestanka drugih primjenjivih ugovora.

Članak 34.

Sankcija za učinjenu povredu odnosno korištenje računalnog informacijskog sustava Općine protivno odredbama ovog Pravilnika ovisit će o vrsti i veličini prekršaja, zatim da li je prekršajem uzrokovana pravna, materijalna ili kakva druga šteta, te radi li se o prvom ili ponovljenom prekršaju.

Sankcije donosi načelnik Općine.

12 Prijelazne i završne odredbe

Članak 35.

Ovaj Pravilnik, zajedno sa pripadajućim procedurama, stupa na snagu danom donošenja, a objavit će se na web stranici Općine Topusko.

Prilagodni period za potpunu primjenu ovog Pravilnika traje šest (6) mjeseci od dana donošenja.

SISAČKO - MOSLAVAČKA ŽUPANIJA
OPĆINA TOPUSKO
OPĆINSKI NAČELNIK

KLASA: 004-02/19-01/02
URBROJ: 2176/18-01-19-1
Topusko, 26. rujna 2019.

OPĆINSKI NAČELNIK

Ivica Kuzmić, v. r.