



REPUBLIKA SRBIJA
OPŠTINA TUTIN
OPŠTINSKA UPRAVA

Broj: IV- 170 /2026

Dana: 01.06.2026.godine

T U T I N

Na osnovu člana 4. stav 8. Zakona o zaposlenima u autonomnim pokrajinama i jedinicama lokalne samouprave ("Sl. glasnik RS", br. 21/2016, 113/2017, 95/2018, 114/2021, 92/2023, 113/2017 - dr. zakon, 95/2018 - dr. zakon, 86/2019 - dr. zakon, 157/2020 - dr. zakon i 123/2021 - dr. zakon), člana 8. Zakona o informacionoj bezbednosti ("Sl. glasnik RS", br. 91/2025), člana 2. Uredbu o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveru bezbednosti informaciono-komunikacionih sistema od posebnog značaja ("Sl. glasnik RS", br. 94/2016) i člana 66. Statuta opštine Tutin („Sl.glasnik opštine Tutin“ br.1/19"), Načelnik opštinske uprave opštine Tutin, donosi

PRAVILNIK

o bezbednosti informaciono-komunikacionog sistema organa opštine Tutin

I. OSNOVNE ODREDBE

Predmet Pravilnika

Član 1.

Ovim pravilnikom bliže se uređuju mere zaštite informaciono-komunikacionog sistema organa opštine Tutin a naročito principi, načini i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema (u daljem tekstu: IKT sistem) kao i ovlašćenja, dužnosti i odgovornosti korisnika informatičkih resursa organa opštine Tutin.

Značenje pojedinih termina

Član 2.

Izrazi upotrebljeni u ovom pravilniku imaju sledeće značenje:

1. IKT sistem je tehnološko-organizaciona celina, koja obuhvata:

- 1) elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije;*
- 2) uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa;*
- 3) podatke koji se vode, čuvaju, obrađuju, pretražuju ili prenose pomoću elektronske komunikacione mreže i uređaja za automatsku obradu podataka, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja;*
- 4) organizacionu strukturu putem koje se upravlja IKT sistemom i*
- 5) sve tipove sistemskog i aplikativnog softvera i softverske razvojne alate;*

2. Mobilni uređaj je elektronski uređaj koji ne mora posedovati sopstvene računarske sposobnosti i koji je bežičan, lako prenosiv, i povezuje se na druge uređaje ili mrežu preko USB porta ili bežičnog protokola (pametni uređaji, nosači podataka kao što su eksterni memorijski nosači podataka i sl);

3. Mere zaštite IKT sistema označavaju sve mere informacione bezbednosti koje se primenjuju u organima opštine Tutin, a tiču se korišćenja IKT sistema, prevencije bezbednosnih incidenata, umanjenja rizika od bezbednosnih incidenata, kao i reakcije u slučaju nastupanja bezbednosnih incidenata, edukacije i drugih mera u cilju obezbeđivanja visokog nivoa informacione bezbednosti u organima opštine Tutin. Merama zaštite se obezbeđuje prevencija od nastanka incidenata i minimizacija štete od incidenata koji ugrožavaju obavljanje delatnosti organa opštine Tutin. Ovim merama se takođe obezbeđuje zaštita podataka sadržanih u IKT sistemu od neovlašćenog pristupa, modifikacije, korišćenja i destrukcije, na način da integritet, tajnost i raspoloživost podataka ne smeju biti kompromitovani;

4. Neophodno da zna (eng. „need to know“) pravilo podrazumeva da korisnik može da ima pristup samo informacijama ili funkcionalnostima IKT sistema koje su neophodne za pravilno izvršenje poslovnih zadataka kao i da pristup informacionim resursima mora biti eksplicitno odobren sa jasnom razlikom između potrebe da se podacima samo pristupi (eng. „read only“) i potrebe da se podaci menjaju (eng.„write“);

5. Nosač podataka je uređaj koji služi za skladištenje ili prenos podataka (diskovi koji su fiksni deo IKT sistema, USB memorije, eksterni diskovi, CD-ovi, DVD-ovi, ostali predmeti i komponente koji imaju mogućnost čuvanja i prenosa podataka);

6. Pametni uređaj je elektronski uređaj koji poseduje sopstvene računarske sposobnosti koji je bežičan, mobilan (lako prenosiv), poseduje jedinstveni ID putem koga se povezuje na druge uređaje ili mrežu preko protokola kao što su Bluetooth, NFC, WiFi, 3G, 4G, 5G i koji prikuplja podatke iz okruženja i ima mogućnost

prosleđivanja podataka drugim uređajima ili krajnjem korisniku. Pod pametnim uređajem u smislu ovog pravilnika smatraju se pametni telefoni, prenosni računari, tableti, mikrokontroleri, pametni satovi i sl.

7. Organi opštine Tutin su Skupština opštine Tutin, Opštinsko veće, uprava opštine Tutin kao i službe i organi koje se osnivaju prema posebnom propisu;

8. Treće lice je pravno ili fizičko lice sa kojim organi opštine sarađuju po osnovu ugovora o održavanju ili implementaciji IKT sistema ili njegovih delova;

9. Korisnik je:

- 1) izabrano, imenovano ili postavljeno lice u organima opštine Tutin (funkcioner);*
- 2) zaposleno lice koje profesionalno obavlja stručne poslove u upravi opštine Tutin na izvršilačkom radnom mestu kao i na radnom mestu službenika na položaju (službenik);*
- 3) lice koje zasniva radni odnos u opštinskoj upravi radi obavljanja pratećih i pomoćno-tehničkih poslova (nameštenik);*
- 4) lice koje je angažovano u upravi opštine Tutin po osnovu ugovora koji podrazumeva rad van radnog odnosa kao što su ugovor o stručnom osposobljavanju, ugovor o privremenim i povremenim poslovima i sl.*

10. kredencijal je struktura podataka koja povezuje identitet nekog korisnika i njegove atribute i šalje se verifikatoru radi provere identiteta i nivoa prava pristupa IKT sistemu (korisničko ime i lozinka, PIN kod, IP adresa, dvofaktorska autentikacija);

11. korisnički nalog čine kredencijali korisnika pomoću koga je korisniku omogućen obim pristupa IKT sistemu u skladu sa poslovima koje obavlja;

12. administratorski nalog čine kredencijali administratora pomoću koga se omogućava administriranje IKT sistema ili njegovih delova.

Ciljevi donošenja Pravilnika

Član 3.

Ciljevi donošenja Pravilnika su:

- 1) određivanje načina i procedura za postizanje i održavanje adekvatnog nivoa informacione bezbednosti u organima opštine Tutin;*
- 2) sprečavanje i ublažavanje posledica incidenata, kojima se ugrožava ili narušava informaciona bezbednost;*

- 3) podizanje svesti kod donosilaca odluka, posebno rukovodilaca organa opštine Tutin i zaposlenih o značaju informacione bezbednosti, rizicima i merama zaštite prilikom korišćenja IKT sistema;*
- 4) propisivanje ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema;*
- 5) sveukupno unapređenje informacione bezbednosti i provera usklađenosti primene mera zaštite u opštini Tutin.*

Obaveza primene Pravilnika

Član 4.

Svi administratori u smislu odredbe čl. 2. st. 1. tač. 7. i korisnici u smislu odredbe čl. 2. st. 1. tač. 4. ovog pravilnika dužni su da primenjuju mere zaštite IKT sistema koje su bliže uređene ovim pravilnikom i koje služe prevenciji nastanka i minimizaciji štete od incidenata. Mere zaštite se primenjuju u svim organima i na svim organizacionim nivoima.

Korisnik se upoznaje sa sadržinom ovog pravilnika prilikom potpisivanja akta koji predstavlja osnov za njegovo angažovanje u organima opštine Tutin i dužan je da postupa u skladu sa njim, kao i u skladu sa drugim internim procedurama kojima se uređuje informaciona bezbednost.

Uz potpisivanje akta iz st. 2. korisnik potpisuje izjavu da je upoznat sa odredbama ovog pravilnika. Jedan primerak ove izjave se čuva u personalnom dosijeu, sa jasno vidljivim datumom potpisivanja.

Predmet zaštite

Član 5.

Predmet zaštite IKT sistema odnosi se na:

- 1) elektronske komunikacione mreže;*
- 2) elektronske uređaje na kojima se čuva i vrši obrada podataka korišćenjem računarskog programa;*
- 3) operativne i aplikativne računarske programe;*
- 4) programski kod;*

- 5) *podatke koji se čuvaju, obrađuju, pretražuju ili prenose pomoću elektronskih uređaja;*
- 6) *organizacionu strukturu putem koje se upravlja IKT sistemom;*
- 7) *korisničke naloge;*
- 8) *informacije za proveru verodostojnosti;*
- 9) *tehničku i korisničku dokumentaciju i*
- 10) *opšte akte i procedure.*

Poslovi IKT bezbednosti

Član 6.

Pod poslovima iz oblasti IKT bezbednosti utvrđuju se:

- 1) *poslovi zaštite informacionih dobara, odnosno sredstava i imovine za nadzor nad poslovnim procesima od značaja za informacionu bezbednost;*
- 2) *poslovi upravljanja rizicima u oblasti informacione bezbednosti, kao i poslovi predviđeni procedurama u oblasti informacione bezbednosti;*
- 3) *poslovi onemogućavanja, odnosno sprečavanja neovlašćene ili nenamerne izmene, oštećenja ili zloupotrebe sredstava, odnosno informacionih dobara IKT sistema opštine Tutin, kao i pristup, izmene ili korišćenje sredstava bez ovlašćenja i bez evidencije o tome;*
- 4) *praćenje aktivnosti, revizije i nadzora u okviru upravljanja informacionom bezbednošću;*
- 5) *obaveštavanje nadležnih organa o incidentima u IKT sistemu, u skladu sa propisima.*

Osnovna pravila bezbednosti informacija

Član 7.

Pri definisanju organizaciono-tehničkih mera zaštite IKT sistema primenjuju se sledeća osnovna pravila:

- 1) *razgraničenje dužnosti;*
- 2) *primena pravila „neophodno da zna“;*
- 3) *procena rizika;*
- 4) *permanentna kontrola i*
- 5) *permanentno usavršanje postojećih rešenja.*

Cilj razgraničenja dužnosti je da se spreče neželjene pojave i incidenti. Ovo se postiže raspodelom zadataka i dodelom korisničkih naloga od kojih je svaki za specifičan poslovni proces.

II. MERE ZAŠTITE IKT SISTEMA

Svrha mera zaštite

Član 8.

Merama zaštite IKT sistema se obezbeđuje prevencija od nastanka incidenata, odnosno prevencija i minimizacija štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti, a posebno u okviru pružanja usluga drugim licima.

1. Uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima korisnika, kojom se ostvaruje upravljanje informacionom bezbednošću u organima opštine Tutin.

Član 9.

Opština Tutin u okviru organizacione strukture utvrđuje poslove i odgovornosti rukovodilaca i zaposlenih u cilju upravljanja informacionom bezbednošću.

Pravilnikom o unutrašnjoj organizaciji i sistematizaciji radnih mesta utvrđuju se radna mesta na kojima se obavljaju poslovi od značaja za obezbeđivanje i praćenje bezbednosti informacionog sistema u svakom od organa opštine Tutin, stepen obuke i kvalifikacija zaposlenih i nivoi pristupa informacionim resursima.

Za nadzor, kontrolu i praćenje primene mera bezbednosti, kao i za proveru da li su podaci zaštićeni na način koji je utvrđen Pravilnikom i internim procedurama usvojenim na osnovu njega, odgovoran je načelnik opštinske uprave i rukovodilac osnovne organizacione jedinice u čijem su delokrugu IKT poslovi (Odsek za informacione tehnologije).

Odgovornost korisnika

Član 10.

Svaki korisnik je odgovoran za bezbednost resursa IKT sistema koje koristi za obavljanje funkcije odnosno poslova radnog mesta.

Pristup IKT sistemu je uslovljen prirodom i karakterom funkcije za izabrana, imenovana i postavljena lica, a u skladu sa propisom koji uređuje njihova prava i obaveze, odnosno u skladu sa zaduženjima i obavezama koje ostali korisnici imaju u skladu sa pravilnikom kojim se uređuju unutrašnja organizacija i sistematizacija, odnosno u skladu sa aktom koji predstavlja osnov za angažovanje korisnika (npr. ugovor o privremenim i povremenim poslovima).

Korisnik pristupa samo onim delovima sistema koji su neophodni za obavljanje njegove funkcije odnosno radnih zadataka u skladu sa pravilom „neophodno da zna“, kako bi se smanjio rizik od zloupotreba, neovlašćenih pristupa, narušavanja integriteta podataka u IKT sistemu i ljudske greške.

Procedurom o pravima pristupa IKT sistemu u organima opštine Tutin utvrđuje se način dodele ovlašćenja za pristup IKT sistemu, način izmene i ukidanja prava pristupa u slučaju kada dođe do promene statusa korisnika kao i postupak zaštite IKT sistema u slučaju gubitka i krađe kredencijala (odnosno parametara za pristup, poput korisničkog imena i lozinke).

Prijava bezbednosnih incidenata

Član 11.

Korisnik je dužan da sve bezbednosne incidente ili probleme prijavi rukovodiocu osnovne organizacione jedinice u čijem su delokrugu IKT poslovi ili zaposlenom u toj jedinici, koga odredi rukovodilac.

Rukovodilac osnovne organizacione jedinice u čijem su delokrugu IKT poslovi bez odlaganja obaveštava načelnika ili rukovodioca organa u kome se dogodio bezbednosni incident ili problem, u zavisnosti od toga da li bezbednosni incident pogađa ceo IKT sistem ili jedan ili više delova i predlaže mere zaštite IKT sistema.

2. Postizanje bezbednosti rada na daljinu i upotreba mobilnih uređaja

Član 12.

Pristup korisnika IKT sistemu van prostorija organa opštine Tutin moguć je u cilju održavanja elektronskih sednica organa, rada na daljinu i rada od kuće.

Neregistrovani korisnici mogu da pristupe putem mobilnih uređaja samo onim delovima sistema koji su konfigurisani tako da omogućavaju pristup internetu ali ne i delovima kroz koje se obavlja službena komunikacija.

Registrovani korisnici imaju pristup resursima IKT sistema putem zaštićene VPN/internet konekcije.

Korisniku je zabranjena samostalna instalacija i podešavanje mobilnog uređaja sa VPN konekcijom kao i davanje uređaja na korišćenje ili servisiranje neovlašćenim licima.

Zaposlenom-korisniku, zabranjena/onemogućena je samostalna instalacija softvera i podešavanje mobilnog uređaja, kao i davanje uređaja drugim neovlašćenim licima (na uslugu, servisiranje i sl.)

Administrator IKT sistema svakodnevno kontroliše pristup resursima IKT sistema i proverava da li ima pristupa sa nepoznatih uređaja (sa nepoznatih MAC adresa). Ukoliko se ustanovi neovlašćen pristup o tome se putem elektronske pošte odmah a najkasnije sledećeg radnog dana obaveštava načelnika opštinske uprave i rukovodioca odseka za informacione tehnologije, a ta se adresa unosi u „block“ listu softvera, koji se koriste za kontrolu pristupa.

Evidenciju privatnih uređaja sa kojih će biti omogućen pristup vodi Administrator IKT sistema, a po odobrenju rukovodioca odseka za informacione tehnologije i načelnika opštinske uprave.

3. Obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost

Član 13.

Načelnik opštinske uprave se stara da zaposleni koji upravljaju IKT sistemom i koji ga koriste budu adekvatno obučeni i imaju svest o značaju adekvatnog korišćenja IKT sistema za poslove koje obavljaju. Njihove odgovornosti se utvrđuju procedurom o pravima pristupa informacionom sistemu, rešenjem o raspoređivanju na određeno radno mesto (za službenike), ugovorom o radu (za nameštenike), posebnim ugovorima (o privremenim i povremenim poslovima i sl.) za radno angažovana lica po drugom osnovu i sporazumom o poverljivosti.

Rukovodilac odseka za informacione tehnologije i Administrator IKT sistema se procedurom o pravima pristupa informacionom sistemu i rešenjem o raspoređivanju ovlašćuju za preduzimanje hitnih i neodložnih mera u slučaju postojanja neposredne opasnosti za podatke i dokumentaciju koje su pod merama zaštite.

U postupku zasnivanja radnog odnosa za zaposlene koji upravljaju IKT sistemom odnosno zaposlene koji koriste IKT sistem u organima opštine Tutin se provode radnje u cilju provere ispunjenosti uslova srazmerno poslovnim zahtevima, klasifikaciji informacija kojima se na radnom mestu koje se popunjava odobrava pristup i sagledanim rizicima.

Svi zaposleni i radno angažovana lica po drugom osnovu, kojima je dodeljen pristup poverljivim informacijama, moraju potpisati sporazum o poverljivosti i zaštiti podataka i informacija od trećih lica, pre nego što im se dozvoli pristup opremi za obradu informacija.

Programima stručnog usavršavanja u opštinskoj upravi se obezbeđuje da se zaposleni koji su nadležni za praćenje, analizu, izveštavanje i preduzimanje aktivnosti na planu sprovođenja usvojene politike i procedura u oblasti informacione bezbednosti kontinuirano obučavaju u cilju unapređenja tehničkog i tehnološkog znanja. Svi službenici opštinske uprave su u obavezi da završe odgovarajuću obuku i redovno stiču nova i obnavljaju postojeća znanja o procedurama koje uređuju bezbednost informacija, na način koji odgovara njihovom poslovnom angažovanju i radnom mestu.

Disciplinski postupak se sprovodi protiv zaposlenih koji su narušili bezbednost informacija ili na drugi način izvršili povredu pravila i politike na snazi i u primeni u opštinskoj upravi. Disciplinski postupak se pokreće po predlogu načelnika opštinske uprave, odnosno rukovodioca odseka za informacione tehnologije.

Službenici i po drugom osnovu angažovana lica, dužni su da čuvaju poverljive i druge informacije koje su od značaja za informacionu bezbednost IKT sistema, nakon prestanka ili promene radnog angažovanja. Dužnosti i obaveze koje ostaju važeće i posle prestanka angažovanja su sadržane u tekstu rešenja o raspoređivanju, ugovora o radu, odnosno ugovora o angažovanju lica van radnog odnosa.

4. Zaštita od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema

Član 14.

Za postupanja prilikom prestanka zaposlenja ili angažovanja zadužen je rukovodilac Odseka za ljudske resurse i lični status građana u saradnji sa službenicima odseka za informacione tehnologije, koji preduzimaju sledeće aktivnosti:

- 1) proveravaju ispunjenost svih uslova u pogledu čuvanja i iznošenja podataka u elektronskom i papirnom formatu;*
- 2) pregledaju sve naloge i pristupe sistemu koji su bili dostupni korisniku, preuzimaju od njega elektronske i druge mobilne uređaje;*
- 3) proveravaju vraćene mobilne uređaje i uređaje za prenošenje podataka;*
- 4) daju nalog za ukidanje naloga elektronske pošte i svih drugih prava pristupa sistemu na dan prestanka radnog odnosa ili drugog osnova angažovanja;*
- 5) pregledaju sve naloge za pristup i prikupljaju pristupne šifre i kodove sa ciljem ukidanja/promene istih na dan odlaska,*
- 6) preuzimaju kartice ili druge uređaje kojima se omogućava pristup poslovnim prostorijama i opremi.*

Promena nivoa odgovornosti, promena radnog mesta ili promena statusa podrazumevaju sprovođenje sveobuhvatne revizije prava pristupa informacionom sistemu, kao da se radi o novom angažovanju (npr. pravo pristupa predmetima kroz ePisarnicu).

5. Identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu

Član 15.

Informaciona dobra opštine Tutin su svi resursi koji sadrže poslovne informacije organa opštine Tutin, odnosno putem kojih se vrši izrada, obrada, čuvanje, prenos, brisanje i uništavanje podataka u IKT sistemu, uključujući sve elektronske zapise, računarsku opremu, mobilne uređaje, baze podataka, poslovne aplikacije, konfiguraciju hardverskih komponenata, tehničku i korisničku dokumentaciju, unutrašnje pravilnike koji se odnose na IKT sistem i sl.

U skladu sa Zakonom o budžetskom sistemu i Uredbom o budžetskom računovodstvu odeljenje za budžet i finansije opštine Tutin u saradnji sa službenicima koji upravljaju IKT sistemom vrši identifikaciju i evidenciju imovine koja je predmet zaštite i dokumentuje njen životni ciklus.

Predmet zaštite su:

- hardverske i softverske komponente IKT sistema
- podaci koji se obrađuju ili čuvaju na komponentama IKT sistema

- korisnički nalozi i drugi podaci o korisnicima informatičkih resursa IKT sistema.

Mere zaštite IKT dobara primenjuju se u skladu sa stepenom osetljivosti i kritičnosti tih dobara, uzimajući u obzir moguće posledice narušavanja poverljivosti, integriteta i raspoloživosti dobara.

6. Klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz Zakona o informacionoj bezbednosti

Član 16.

Klasifikovanje podatka je postupak utvrđivanja i pojedinačnog dodeljivanja nivoa tajnosti podatka, u skladu sa njihovim značajem. Klasifikaciona šema poverljivosti informacija je zasnovana na četiri nivoa:

- 1) otkrivanje ne izaziva nikakvu štetu;*
- 2) otkrivanje izaziva manju neprijatnost ili manju štetu;*
- 3) otkrivanje ima značajan kratkoročni uticaj na obavljanje poslova iz delokruga organa opštine Tutin;*
- 4) otkrivanje ima ozbiljan uticaj na dugoročne strateške ciljeve ili obavljanje poslova iz delokruga organa opštine Tutin.*
- 5) Organi opštine Tutin vrše klasifikaciju radi:*
 - *jačanja korisničke odgovornosti, kako bi korisnici mogli da uoče i prepoznaju poslovnu vrednost podatka prilikom čuvanja ili slanja i postanu svesni odgovornosti za neovlašćeno korišćenje ili prenošenje;*
 - *podizanja svesti o vrednosti informacije ili dokumenta;*
 - *zaštite podataka u pokretu radi bolje i inteligentnije integracije sa DLP, WEB gateway i ostalim proizvodima za zaštitu parametara i krajnjih uređaja.*
- 6) Podaci koji se nalaze u IKT sistemu predstavljaju tajnu, ako su tako definisani odredbama posebnim propisima.*
- 7) Podaci koji se označe kao tajni, moraju biti zaštićeni u skladu sa odredbama Uredbe o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima („Sl. glasnik RS", br. 53/2011 55/05, 71/05 – ispravka, 101/07, 65/08 i 16/11).*

Detaljan opis informacija, nosačima informacija i dostupnosti podataka nalazi se u Informatoru o radu opštine Tutin.

7. Zaštita nosača podataka

Član 17.

Odsek za informacione tehnologije će uspostaviti organizaciju pristupa i rada sa podacima, posebno onima koji budu označeni stepenom službenosti ili tajnosti u skladu sa Zakonom o tajnosti podataka, tako da:

- 1) podaci i dokumenti (posebno oni sa oznakom tajnosti) mogu da se snime (arhiviraju, zapišu) na serveru na kome se snimaju podaci, u folderu nad kojim će pravo pristupa imati samo korisnici kojima je to pravo obezbeđeno aktom koji određuje prava pristupa;
- 2) podaci i dokumenti sa oznakom tajnosti mogu da se snime na druge nosače (eksterni hard disk, USB, CD, DVD) samo od strane ovlašćenih službenika iz odseka za informacione tehnologije

Evidenciju nosača podataka na kojima su snimljeni podaci, vodi odsek za informacione tehnologije i ti nosači moraju biti propisno obeleženi i odloženi na mesto na kome će biti zaštićeni od neovlašćenog pristupa.

U slučaju transporta nosača podataka, načelnik opštinske uprave će odrediti odgovornu osobu i način transporta.

U slučaju isteka rokova čuvanja podataka koji se nalaze na nosačima, podaci moraju biti nepovratno obrisani, a ako to nije moguće, takvi nosači podataka moraju biti fizički oštećeni, odnosno uništeni.

Obavezno je minimizovati korišćenja nosača podataka. Pre korišćenja nosači podataka moraju se podvrgnuti proverbi sredstvima za zaštitu od zlonamernog softvera.

Obavezno je pouzdano uništenje podataka sa nosača podataka koji se ne koriste više od godinu dana. U slučaju nemogućnosti pouzdanog uništenja podataka mora se obaviti fizičko uništenje nosača.

8. Ograničenje pristupa podacima i sredstvima za obradu podataka

Član 18.

Pristup resursima IKT sistema određen je vrstom naloga, odnosno dodeljenom ulogom koju korisnik ima.

Korisnik koji ima administratorski nalog, ima prava pristupa svim resursima IKT sistema (softverskim i hardverskim, mreži i mrežnim resursima) u cilju instalacije, održavanja, podešavanja i upravljanja resursima IKT sistema.

Korisnik može da koristi samo svoj korisnički nalog koji je dobio od administratora i ne sme da omogući drugom licu korišćenje njegovog korisničkog naloga, sem administratoru za podešavanje korisničkog profila i radne stanice.

Korisnik koji na bilo koji način zloupotrebi prava, odnosno resurse IKT sistema, podleže krivičnoj i disciplinskoj odgovornosti.

Korisnik je dužan da poštuje i sledeća pravila bezbednog i primerenog korišćenja resursa IKT sistema, i to da:

- 1) koristi informatičke resurse isključivo u poslovne svrhe;*
- 2) prihvati da su svi podaci koji se skladište, prenose ili procesiraju u okviru informatičkih resursa vlasništvo organa opštine Tutin i da mogu biti predmet nadgledanja i pregledanja;*
- 3) postupa sa poverljivim podacima u skladu sa propisima, a posebno prilikom kopiranja i prenosa podataka;*
- 4) bezbedno čuva svoje lozinke, odnosno da ih ne odaje drugim licima;*
- 5) menja lozinke saglasno utvrđenim pravilima;*
- 6) pre svakog udaljavanja od radne stanice, odjavi se sa sistema, odnosno zaključa radnu stanicu*
- 7) zahtev za instalaciju softvera ili hardvera podnosi u pisanoj formi, odobren od strane neposrednog rukovodioca;*

- 8) obezbedi sigurnost podataka u skladu sa važećim propisima;*
- 9) pristupa informatičkim resursima samo na osnovu eksplicitno dodeljenih korisničkih prava;*
- 10) ne sme da zaustavlja rad ili briše antivirusni program, menja njegove podešene opcije, niti da neovlašćeno instalira drugi antivirusni program;*
- 11) na radnoj stanici ne sme da skladišti sadržaj koji ne služi u poslovne svrhe;*
- 12) izrađuje zaštitne kopije (backup) podataka u skladu sa propisanim procedurama;*
- 13) koristi internet i elektronsku poštu u organima opštine Tutin u skladu sa propisanim procedurama;*
- 14) prihvati da se određene vrste informatičkih intervencija (izrada zaštitnih kopija, ažuriranje programa, pokretanje antivirusnog programa i sl.) obavljaju u utvrđeno vreme;*
- 15) prihvati da svi pristupi informatičkim resursima i informacijama treba da budu zasnovani na principu minimalne neophodnosti;*
- 16) prihvati da tehnike sigurnosti (anti virus programi, firewall, sistemi za detekciju upada, sredstva za šifriranje, sredstva za proveru integriteta i dr.) sprečavaju potencijalne pretnje IKT sistemu.*
- 17) ne sme da instalira, modifikuje, isključuje iz rada ili briše zaštitni, sistemski ili aplikativni softver, osim ako to nije sklopu održavanja sistema ili otklanjanja problema, uz saglasnost nadređenog.*

9. Odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža

Član 19.

Pravo pristupa imaju samo korisnici koji imaju administratorske ili korisničke naloge.

Administratorski nalog je jedinstveni nalog kojim je omogućen pristup i administracija svih resursa IKT sistema, kao i otvaranje novih i izmena postojećih naloga.

Administratorski nalog mogu da koriste samo zaposleni u odseku za informacione tehnologije.

Administratorski nalog za upravljanje domenom i upravljanje bazama podataka mogu da koriste samo zaposleni u odseku za informacione tehnologije.

Korisnički nalog se sastoji od korisničkog imena i lozinke, koji se mogu ukucavati ili čitati sa nosača podataka na kome postoji elektronski sertifikat, na osnovu koga se vrši autentikacija – provera identiteta i autorizacija – provera prava pristupa, odnosno prava korišćenja resursa IKT sistema od strane korisnika.

Korisnički nalozi su jedinstveni, tako da se korisnici mogu vezati uz njih i učiniti odgovornim za svoje aktivnosti. Korisnički nalog dodeljuje administrator, na osnovu zahteva službenika zaduženog za upravljanje ljudskim resursima u saradnji sa neposrednim rukovodiocem i to tek nakon unosa podataka o zaposlenom u softver za upravljanje ljudskim resursima, a u skladu sa potrebama obavljanja poslovnih zadataka od strane korisnika. Svakom korisniku se dodeljuje pravo pristupa IKT sistemu u skladu sa radnim zadacima koje obavlja. Korisniku se dodeljuju jedinstveni podaci za logovanje i jedinstvena šifra za logovanje, koji se ne smeju deliti sa drugim korisnicima.

Administrator vodi evidenciju o korisničkim nalogima, proverava njihovo korišćenje, menja prava pristupa i ukida korisničke naloge na osnovu zahteva službenika na poslovima upravljanja ljudskim resursima, odnosno nadležnog rukovodioca.

Korišćenje zajedničkih identifikatora dozvoljava se samo onda kada je to pogodno za obavljanje posla uz prethodno odobrenje. Korisnicima kojima je prestao radni odnos ili period angažovanja trenutno se onemogućavaju ili uklanjaju korisnički nalozi. Korisniku se dodeljuju jedinstveni podaci za logovanje i jedinstvena šifra za logovanje, koji se ne smeju deliti sa drugim korisnicima. Administrator IKT sistema svakih 12 meseci vrši preispitivanje prava korisnika na pristup, kao i nakon svake promene (unapređenje, razrešenje i kraj zaposlenja).

Redovne poslovne aktivnosti se ne vrše iz privilegovanih korisničkih naloga. Kompetencije korisnika sa privilegovanim pravima na pristup se redovno preispituju radi provere da li su u skladu sa njihovim obavezama.

10. Utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju

Član 20.

Korisnički nalog se sastoji od korisničkog imena i lozinke.

Lozinka mora da sadrži minimum osam karaktera kombinovanih od malih i velikih slova, cifara i specijalnih znakova.

Lozinka ne sme da sadrži ime, prezime, datum rođenja, broj telefona i druge prepoznatljive podatke.

Ako korisnik posumnja da je drugo lice otkrilo njegovu lozinku dužan je da istu odmah izmeni.

Korisnik dužan je da menja lozinku najmanje jednom u šest meseci.

Ista lozinka se ne sme ponavljati u vremenskom periodu od godinu dana.

Korisnički nalog može da se kreira i na osnovu podataka koji se nalaze na mediju sa kvalifikovanim elektronskim sertifikatom (npr. lična karta sa čipom i upisanim sertifikatom).

Prijavljivanje u IKT sistem opštine Tutin se vrši ubacivanjem nosača podataka sa elektronskim sertifikatom u čitač kartica.

Neovlašćeno ustupanje korisničkog naloga drugom licu, podleže disciplinskoj odgovornosti.

11. Predviđanje odgovarajuće upotrebe kriptozastite radi zaštite tajnosti, autentičnosti odnosno integriteta podataka

Član 21.

Pristup resursima IKT sistema organa opštine Tutin ne zahteva posebnu kriptozastitu. Kriptozastita se primenjuje u skladu sa procenom rizika i tehničkim mogućnostima sistema.

Korisnici koriste kvalifikovane elektronske sertifikate za elektronsko potpisivanje dokumenata kao i autentikaciju i autorizaciju pristupa pojedinim aplikacijama.

Službenici na poslovima IKT su zaduženi za instalaciju potrebnog softvera i hardvera za korišćenje sertifikata.

Korisnici su dužni da čuvaju svoje kvalifikovane elektronske sertifikate kako ne bi došli u posed drugih lica.

12. Fizička zaštita objekata, prostora, prostorija odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu

Član 22.

U opštini Tutin se obezbeđuje i primenjuje odgovarajuća kontrola pristupa, čime se omogućava fizička bezbednost kancelarija, prostorija i sredstava. Takođe, bezbednim konfigurisanjem se onemogućava pristup ključnoj opremi a u cilju sprečavanja vidljivosti poverljivih informacija, aktivnostima spolja.

Prostor u kome se nalaze serveri, mrežna ili komunikaciona oprema IKT sistema, organizuje se kao bezbednosna zona. Bezbednosna zona se uspostavlja za fizički pristup resursima IKT sistema u kontrolisanom, vidljivo označenom prostoru, koji je obezbeđen mehaničkom bravom i video nadzorom.

Bezbednosne zone su zaštićene odgovarajućim kontrolama ulaska kako bi se osiguralo da je samo ovlašćenim pojedincima dozvoljen pristup. U bezbednosnoj zoni se održava i vrši provera svih pristupa.

Prostor bezbednosne zone je obezbeđen od kompromitujućeg elektromagnetnog zračenja (KEMZ), požara i drugih elementarnih nepogoda, i u njemu je osigurano održavanje odgovarajuće temperature (grejanje odnosno hlađenje/klimatizacija).

Evidenciju o ulasku u ovu zonu vodi odsek za informacione tehnologije.

13. Zaštita od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem

Član 23.

Ulaz u prostoriju u kojoj se nalazi IKT oprema, dozvoljen je samo administratoru IKT sistema odnosno službenicima odseka za informacione tehnologije.

Osim administratora sistema, pristup administrativnoj zoni mogu imati i treća lica u cilju instalacije i servisiranja određenih resursa IKT sistema, a po prethodnom odobrenju načelnika opštinske uprave uz prisustvo službenika odseka za informacione tehnologije.

Pristup bezbednosnoj zoni može imati i zaposleni na poslovima održavanja higijene uz prisustvo nadležnog lica.

Prostorija mora biti vidljivo obeležena i u njoj se mora nalaziti protivpožarna oprema, koja se može koristiti samo u slučaju požara u prostoriji u kojoj se nalazi IKT oprema i nosači podataka.

Prozori i vrata na ovoj prostoriji moraju uvek biti zatvoreni, i po potrebi obezbeđeni rešetkom.

Serveri i aktivna mrežna oprema (switch, modem, router, firewall), moraju stalno biti priključeni na uređaje za neprekidno napajanje – UPS.

U slučaju nestanka električne energije, u periodu dužem od kapaciteta UPS-a, ovlašćeno lice je dužno da isključi opremu u skladu sa procedurama proizvođača opreme.

IKT oprema iz prostorije se u slučaju opasnosti (požar, vremenske nepogode i sl.) može izneti i bez odobrenja načelnika opštinske uprave.

U slučaju iznošenja opreme radi selidbe, ili servisiranja, neophodno je odobrenje načelnika opštinske uprave, koji će odrediti uslove, način i mesto iznošenja opreme.

Ako se oprema iznosi radi servisiranja, pored odobrenja načelnika opštinske uprave, potrebno je sačiniti zapisnik u kome se navodi naziv i tip opreme, serijski broj, naziv serviser, ime i prezime ovlašćenog lica serviser.

Ugovorom sa serviserom mora biti definisana obaveza zaštite podataka koji se nalaze na nosačima podataka koji su deo IKT resursa opštine Tutin.

14. Obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka

Član 24.

Službenici na poslovima IKT kontinuirano nadziru i proveravaju funkcionisanje sredstava za obradu podataka i upravljaju rizicima koji mogu uticati na bezbednost IKT sistema i, u skladu sa tim, planiraju, odnosno predlažu načelniku opštinske uprave odgovarajuće mere.

Pre uvođenja u rad novog softvera neophodno je napraviti kopiju-arhivu postojećih podataka, u cilju pripreme za proceduru vraćanja na prethodnu stabilnu verziju.

Instaliranje novog softvera kao i ažuriranje postojećeg, odnosno instalacija nove verzije, može se vršiti na način koji ne ometa operativni rad korisnika.

U slučaju da se na novoj verziji softvera koji je uveden u operativni rad primete bitni nedostaci koji mogu uticati na rad, potrebno je primeniti proceduru za vraćanje na prethodnu stabilnu verziju softvera.

Za razvoj i testiranje softvera pre uvođenja u rad u IKT sistem moraju se koristiti serveri i podaci koji su namenjeni testiranju i razvoju.

Pri testiranju softvera je potrebno obezbediti neometano funkcionisanje IKT sistema. Zabranjeno je korišćenje servera koji se koriste u operativnom radu za testiranje softvera, na način koji može da zaustavi normalno funkcionisanje IKT sistema.

15. Zaštita podataka i sredstva za obradu podataka od zlonamernog softvera

Član 25.

Zaštita od zlonamernog softvera na mreži sprovodi se u cilju zaštite od virusa i druge vrste zlonamernog koda koji u računarsku mrežu mogu dospeti internet konekcijom, imejlom, zaraženim nosačima podataka (USB memorija, CD itd.), instalacijom nelicenciranog softvera i sl.

Za uspešnu zaštitu od virusa na svakom računaru je instaliran antivirusni program. Antivirusne definicije se redovno automatski ažuriraju.

Svakog radnog dana u nedelji je potrebno ostaviti uključene i zaključane računare radi skeniranja na viruse.

Zabranjeno je zaustavljanje i isključivanje antivirusnog softvera tokom skeniranja nosača podataka.

Nosači podataka, pre korišćenja, moraju biti provereni na prisustvo virusa. Ako se utvrdi da nosač podataka sadrži viruse, ukoliko je to moguće, vrši se čišćenje nosača podataka antivirusnim softverom.

Rizik od eventualnog gubitka podataka prilikom čišćenja nosača podataka od virusa snosi donosilac nosača podataka.

Rukovodioci organizacionih jedinica određuju koji zaposleni imaju pravo pristupa internetu radi prikupljanja podataka i ostalih informacija vezanih za obavljanje poslova u njihovoj nadležnosti.

Korisnicima koji su priključeni na IKT sistem je zabranjeno samostalno priključivanje na internet (priključivanje preko sopstvenog modema), pri čemu Administrator sistema može ukinuti pristup internetu u slučaju dokazane zloupotrebe istog.

Korisnici IKT sistema koji koriste internet moraju da se pridržavaju mera zaštite od virusa i upada sa interneta u IKT sistem, a svaki računar čiji se korisnik priključuje na Internet mora biti odgovarajuće podešen i zaštićen, pri čemu podešavanje vrši Administrator sistema.

Prilikom korišćenja interneta treba izbegavati sumnjive WEB stranice, s obzirom da to može prouzrokovati probleme - neprimetno instaliranje špijunskih programa i slično.

U slučaju da korisnik primeti neobično ponašanje računara, zapažanje treba bez odlaganja da prijavi Administratoru sistema.

Strogo je zabranjeno gledanje filmova i igranje igrice na računarima i "krstarenje" WEB stranicama koje sadrže nedoličan sadržaj, kao i samovoljno preuzimanje istih sa interneta.

Nedozvoljena upotreba interneta obuhvata:

- instaliranje, distribuciju, oglašavanje, prenos ili na drugi način činjenje dostupnim „piratskih“ ili drugih softverskih proizvoda koji nisu licencirani na odgovarajući način;
- narušavanje sigurnosti mreže ili na drugi način onemogućavanje poslovne internet komunikacije;
- namerno širenje destruktivnih i opstruktivnih programa na internetu (internet virusi, internet trojanski konji, internet crvi i druge vrste malicioznih softvera);

- nedozvoljeno korišćenje društvenih mreža i drugih internet sadržaja koje je ograničeno;
- preuzimanje (download) podataka velike "težine" koje prouzrokuje "zagušenje" na mreži;
- preuzimanje (download) materijala zaštićenih autorskim pravima;
- korišćenje linkova koji nisu u vezi sa poslom (gledanje filmova, audio i videostreaming i sl.);
- nedozvoljeni pristup sadržaju, promena sadržaja, brisanje ili prerada sadržaja preko interneta.

Korisnicima koji neadekvatnim korišćenjem interneta uzrokuju zagušenje, prekid u radu ili narušavaju bezbednost mreže može se oduzeti pravo pristupa.

Lista provera u cilju zaštite od zlonamernog softvera

Član 26.

Lista provera koje se sprovode u cilju zaštite od zlonamernog softvera obuhvata ali se ne ograničava na:

a) proveru, pre korišćenja, svih datoteka na elektronskim ili optičkim uređajima, kao i datoteka primljenih preko mreža, da li sadrže zlonamerni softver;

b) proveru, pre korišćenja, sadržaja priloga elektronske pošte i preuzetih sadržaja, da li sadrže zlonamerni softver; ova provera se sprovodi na raznim mestima, npr. na serverima za elektronsku poštu, na stonim računarima ili prilikom ulaska u mrežu operatora IKT sistema;

v) proveru postojanja zlonamernih softvera na veb-stranicama;

g) obuka za izveštavanje i oporavak od napada zlonamernim softverom;

d) pripremu odgovarajućih planova za kontinuitet poslovanja prilikom oporavka od napada zlonamernim softverom, uključujući sve neophodne rezervne kopije podataka i softvera i mehanizme za oporavak;

đ) implementaciju procedura za redovno prikupljanje informacija, kao što je pretplata na adresne spiskove za dostavu ili provera veb-stranica na kojima se daju informacije o novim zlonamernim softverima;

e) implementaciju procedura za verifikovanje informacija o zlonamernim softverima i obezbeđenje da su upozoravajući izveštaji tačni i informativni; za razlikovanje lažnih

od stvarnih zlonamernih softvera koriste se kvalifikovani izvori, npr. provereni časopisi, pouzdane stranice na Internet mreži ili isporučioi programa protiv zlonamernih softvera.

16. Zaštita od gubitka podataka

Član 27.

Rezervne kopije informacija, softvera i duplikati sistema se redovno izrađuju i ispituju. Zaštitne kopije korisnicima obezbeđuju korisničke podatke, funkcionalnost servisa i aplikacija nakon uništenja ili oštećenja koja su nastala usled hakerskih napada, otkaza hardvera, grešaka korisnika, prirodnih katastrofa i drugih nesreća.

Pod zaštitnim kopijama podrazumeva se pravljenje rezervnih kopija korisničkih podataka, konfiguracionih i log fajlova, kritičnih fajlova za funkcionisanje operativnih sistema (serverskih, korisničkih i komunikacionih) ili celih operativnih sistema, aplikacija, servisa i baze podataka.

Zaštitne kopije treba da omoguće brzo i efikasno vraćanje u funkciju sistema u slučaju neželjenih događaja, i treba ih praviti u vreme kada se ne umanjuje raspoloživost servisa, aplikacija, baza podataka i komunikacionih kapaciteta IKT sistema. Za čuvanje zaštitnih kopija koriste se eksterni hard diskovi i CD/DVD nosači podataka.

Dnevno kopiranje-arhiviranje vrši se za svaki radni dan u sedmici, od 20 časova svakog radnog dana.

Nedeljno kopiranje-arhiviranje vrši se poslednjeg radnog dana u nedelji, od 21 čas.

Mesečno kopiranje-arhiviranje vrši se poslednjeg radnog dana u mesecu, za svaki mesec posebno, od 22 časa.

Godišnje kopiranje-arhiviranje vrši se poslednjeg radnog dana u godini.

Svaki primerak godišnje kopije-arhive čuva se u roku koji je definisan Uputstvom o kancelarijskom poslovanju organa državne uprave („Sl. glasnik RS“, br 10/93, 14/93-ispr, 67/2016 i 3/2017).

Svaki primerak nosača podataka sa kopijama-arhivama, mora biti označen brojem, vrstom (dnevna, nedeljna, mesečna, godišnja), datumom izrade kopije-arhive, kao i imenom korisnika koji je izvršio kopiranje-arhiviranje.

Dnevne, nedeljne i mesečne kopije-arhive se čuvaju u bezbednosnoj zoni.

Godišnje kopije-arhive se izrađuju u dva primerka, od kojih se jedan čuva u prostoriji u kojoj se čuvaju dnevne, nedeljne i mesečne kopije-arhive a drugi primerak na izdvojenoj lokaciji koju odredi načelnik opštinske uprave.

17. Čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema

Član 28.

O aktivnostima administratora i korisnika vode se dnevници aktivnosti (activitylog, history, securitylog, transactionlog i dr).

Svakog poslednjeg radnog dana u nedelji datoteke u kojima se nalazi dnevnik aktivnosti se arhiviraju po proceduri za izradu kopija-arhiva ostalih podataka u IKT sistemu, u skladu sa čl. 27 ovog pravilnika.

Sistem za kontrolu i dojavu o greškama, neovlašćenim aktivnostima i dr, mora biti podešen tako da odmah obaveštava sistem administratora, rukovodioca odseka za informacione tehnologije i načelnika opštinske uprave, o svim neregularnim aktivnostima korisnika, pokušajima upada i upadima u sistem.

18. Obezbeđivanje integriteta softvera i operativnih sistema

Član 29.

U IKT sistemu može da se instalira samo softver za koji postoji važeća licenca u vlasništvu opštine Tutin, odnosno Freeware i Opensource verzije.

Instalaciju i podešavanje softvera može da vrši samo zaposleni odseka za informacione tehnologije, odnosno korisnik koji ima ovlašćenje za to.

Instalaciju i podešavanje softvera može da izvrši i treće lice, u skladu sa Ugovorom o nabavci, odnosno održavanju softvera.

Pre svake instalacije nove verzije softvera, odnosno podešavanja, neophodno je napraviti kopiju postojećeg, kako bi se obezbedila mogućnost povratka na prethodno stanje u slučaju neočekivanih situacija.

19. Zaštita od zloupotrebe bezbednosnih slabosti IKT sistema

Član 30.

Administrator sistema najmanje jednom mesečno a po potrebi i češće vrši analizu dnevnika aktivnosti (activitylog, history, securitylog, transactionlog i dr) u cilju identifikacije potencijalnih slabosti IKT sistema.

Ukoliko se identifikuju slabosti koje mogu da ugroze bezbednost IKT sistema, Administrator sistema je dužan da odmah izvrši podešavanja, odnosno instalira softver koji će otkloniti uočene slabosti.

Administrator sistema treba da podešavanjem korisničkih polisa, onemogući neovlašćeno instaliranje softvera koji može dovesti do ugrožavanja bezbednosti IKT sistema.

20. Obezbeđivanje da aktivnosti na reviziji IKT sistema imaju što manji uticaj na funkcionisanje sistema

Član 31.

Revizija IKT sistema se mora vršiti tako da ima što manji uticaj na poslovne procese korisnika. Ukoliko to nije moguće u radno vreme, onda se vrši nakon završetka radnog vremena korisnika, čiji bi poslovni proces bio ometan, uz prethodnu saglasnost načelnika Uprave.

21. Zaštita podataka u komunikacionim mrežama uključujući uređaje i vodove

Član 32.

Komunikacioni kablovi i kablovi za napajanje moraju biti postavljeni u zidu ili kanalicama, tako da se onemogući neovlašćen pristup, odnosno da se izvrši izolacija od mogućeg oštećenja.

Mrežna oprema (switch, router, firewall) se mora nalaziti u zaključanom rack ormanu.

Administrator sistema je dužan da stalno vrši kontrolni pregled mrežne opreme i blagovremeno preduzima mere u cilju otklanjanja eventualnih nepravilnosti.

Bežična mreža koju mogu da koriste posetioци objekata u nadležnosti organa opštine Tutin, mora biti odvojena od interne mreže koju koriste korisnici u organima opštine Tutin i kroz koju se vrši razmena službenih podataka.

22. Bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT sistema

Član 33.

Razmena podataka koji se prenose unutar operatora IKT sistema biće definisana posebnim protokolom.

23. Pitanja informacione bezbednosti u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema

Član 34.

Način instaliranja novih, zamena i održavanje postojećih resursa IKT sistema od strane trećih lica koja nisu zaposlena u organima opštine Tutin, biće definisan ugovorom koji će biti sklopljen sa tim licima.

Administrator sistema je zadužen za tehnički nadzor nad realizacijom ugovorenih obaveza od strane trećih lica.

O uspostavljanju novog IKT sistema, odnosno uvođenju novih delova i izmenama postojećih delova IKT sistema Administrator sistema vodi dokumentaciju.

Dokumentacija iz prethodnog stava mora da sadrži opise svih procedura a posebno procedura koje se odnose na bezbednost IKT sistema.

24. Zaštita podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova sistema

Član 35.

Za potrebe testiranja IKT sistema odnosno delova sistema odsek za informacione tehnologije može da koristi podatke koji nisu osetljivi, koje štiti, čuva i kontroliše na odgovarajući način.

25. Zaštita sredstava operatora IKT sistema koja su dostupna pružaocima usluga

Član 36.

Treća lica-pružaoci usluga izrade i održavanja softvera mogu pristupiti samo onim podacima koji se nalaze u bazama podataka koje su deo softvera koji su oni izradili, odnosno za koje postoji ugovorom definisan pristup.

Administrator sistema je odgovoran za kontrolu pristupa i nadzor nad izvršenjem ugovorenih obaveza, kao i za poštovanje odredbi ovog pravilnika kojima su takve aktivnosti definisane.

Pre otpočinjanja pregovora, potencijalni pružalac usluga u obavezi je da potpiše izjavu o poverljivosti i zaštiti podataka, informacija i dokumentacije, koja sadrži obavezu za pružaoca usluga da dostavljene ili na drugi način učinjene dostupnim informacije i podaci mogu biti korišćeni isključivo na način prethodno odobren od strane ovlašćenog lica, a za potrebe izvršenja predmeta pregovora.

Izjava o poverljivosti, odnosno ugovor o pružanju usluga, sadrži odredbu o poverljivosti sa jasno utvrđenom obavezom i odgovornošću pružaoca usluge uz pretnju raskida ugovora i naknade štete u korist opštine Tutin u slučaju povrede ove odredbe.

Izjava o poverljivosti obavezno glasi:

“Svi podaci i informacije sadržani u ovom Ugovoru o pružanju usluga se smatraju poverljivim poslovnim podacima i ne smeju biti saopšteni ili na drugi način učinjeni dostupnim trećim licima. Naročito se smatraju poverljivim svi poslovni podaci i informacije koje jedna strana učini dostupnim drugoj ugovornoj strani radi izvršenja obaveza iz ovog ugovora, ukoliko ti podaci nisu javno dostupni niti su bili prethodno poznati drugoj strani.

Svaka ugovorna strana se obavezuje da podatke i informacije koje joj budu učinjene dostupnim u skladu sa ovim ugovorom i obavezom izvršenja ugovorenih poslova i obaveza, budu stavljene na raspolaganje i uvid zaposlenima, ukoliko je to neophodno radi izvršenja obaveza iz ovog ugovora.

Ugovorne strane se naročito obavezuju da postupaju obazrivo sa podacima o ličnosti do kojih mogu doći u postupku izvršenja usluga za operatora IKT sistema, kao i da te podatke čuvaju i postupaju u svemu u skladu sa propisima koji uređuju zaštitu podataka o ličnosti.

U slučaju povrede ove obaveze ugovorna strana čiji su podaci korišćeni ima pravo raskida ugovora i pravo da zahteva naknadu štete usled neovlašćenog korišćenja podataka i informacija druge strane.”

Pružaoци usluga dužni su da zahteve opštine Tutin u pogledu bezbednosti informacija prošire i na svoje podugovarače za dodatne usluge ili proizvode.

Administrator sistema je odgovoran za kontrolu pristupa i nadzor nad izvršenjem ugovorenih obaveza, kao i za poštovanje odredbi pravilnika kojima su takve aktivnosti definisane.

26. Održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga

Član 37.

Rukovodilac odseka za informacione tehnologije je odgovoran za nadzor nad poštovanjem ugovorenih obaveza od strane trećih lica-pružaoca usluga, posebno u oblasti poštovanja odredbi kojima je definisana bezbednost resursa IKT sistema. U slučaju nepoštovanja ugovorenih obaveza rukovodilac odseka za informacione tehnologije je dužan da odmah obavesti načelnika opštinske uprave, kako bi on mogao da preduzme mere u cilju otklanjanja nepravilnosti.

27. Prevencija i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama

Član 38.

U slučaju bilo kakvog incidenta koji može da ugrozi bezbednost resursa IKT sistema, korisnik je dužan da odmah obavesti Administratora sistema.

Po prijemu prijave, Administrator sistema je dužan da odmah obavesti načelnika opštinske uprave i preduzme mere u cilju zaštite resursa IKT sistema.

Ukoliko se radi o incidentu koji je definisan u skladu sa Uredbom o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja, „Sl. glasnik RS“, br, 94/2016), Administrator sistema, je dužan da pored načelnika opštinske uprave obavesti i nadležni organ definisan ovom uredbom.

Administrator sistema vodi evidenciju o svim incidentima, kao i prijavama incidenata, u skladu sa uredbom, na osnovu koje, protiv odgovornog lica, mogu da se vode disciplinski, prekršajni ili krivični postupci.

28. Mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima

Član 39.

U slučaju vanrednih okolnosti, koje mogu da dovedu do izmeštanja IKT sistema iz zgrade Uprave, Administrator sistema je dužan da u najkraćem roku prenese delove IKT sistema neophodne za funkcionisanje u vanrednoj situaciji na rezervnu lokaciju, u skladu sa planom reagovanja u vanrednim i kriznim situacijama.

Specifikaciju delova IKT sistema koji su neophodni za funkcionisanje u vanrednim situacijama izrađuje odsek za informacione tehnologije, i to u tri primerka, od kojih se jedan nalazi kod njega, drugi kod zaposlenog nadležnog za poslove odbrane i vanredne situacije a treći primerak kod načelnika opštinske uprave.

Delove IKT sistema koji nisu neophodni za funkcionisanje u vanrednim situacijama, skladište se na rezervnu lokaciju, koju odredi načelnik opštinske uprave. Skladištenje delova IKT sistema koji nisu neophodni, se vrši tako da oprema bude bezbedna i obeležena, u skladu sa evidencijom koja se o njoj vodi.

Izmena Pravilnika o bezbednosti

Član 40.

U slučaju nastanka promena koje mogu nastupiti usled tehničko-tehnoloških, kadrovskih, organizacionih promena u IKT sistemu i događaja na globalnom i nacionalnom nivou koji mogu narušiti informacionu bezbednost, rukovodilac odseka za informacione tehnologije je dužan da obavesti načelnika opštinske uprave, kako bi on mogao da pristupi izmeni ovog pravilnika, u cilju unapređenja mera zaštite, načina i procedura postizanja i održavanja adekvatnog nivoa bezbednosti IKT sistema, kao i preispitivanje ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema.

Provera IKT sistema

Član 41.

Proveru IKT sistema vrši Administrator sistema vrši načelnik Opštinske uprave na osnovu izveštaja koji sačinjava administrator.

Provera se vrši tako što se:

- 1) proverava usklađenost Pravilnika o bezbednosti IKT sistema, uzimajući u obzir i pravilnike na koja se vrši upućivanje, sa propisanim uslovima, odnosno proverava da li su pravilnikom adekvatno predviđene mere zaštite, procedure, ovlašćenja i odgovornosti u IKT sistemu;*
- 2) proverava da li se u operativnom radu adekvatno primenjuju predviđene mere zaštite i procedure u skladu sa utvrđenim ovlašćenjima i odgovornostima, metodama intervjua, simulacije, posmatranja, uvida u predviđene evidencije i drugu dokumentaciju;*
- 3) vrši provera bezbednosnih slabosti na nivou tehničkih karakteristika komponenti IKT sistema metodom uvida u izabrane proizvode, arhitekture rešenja, tehničke konfiguracije, tehničke podatke o statusima, zapise o događajima (logove) kao i metodom testiranja postojanja poznatih bezbednosnih slabosti u sličnim okruženjima.*

O izvršenoj proveru sačinjava se izveštaj, koji se dostavlja načelniku opštinske uprave.

Sadržaj izveštaja o proveru IKT sistema

Član 42.

Izveštaj o proveru IKT sistema sadrži:

- 1) naziv operatora IKT sistema koji se proverava;*
- 2) vreme provere;*
- 3) podaci o licima koja su vršila proveru;*

- 4) izveštaj o sprovedenim radnjama provere;*
- 5) zaključke po pitanju usklađenosti Pravilnika o bezbednosti IKT sistema sa propisanim uslovima;*
- 6) zaključke po pitanju adekvatne primene predviđenih mera zaštite u operativnom radu;*
- 7) zaključke po pitanju eventualnih bezbednosnih slabosti na nivou tehničkih karakteristika komponenti IKT sistema;*
- 8) ocena ukupnog nivoa informacione bezbednosti;*
- 9) predlog eventualnih korektivnih mera;*
- 10) potpis odgovornog lica koje je sprovelo proveru IKT sistema.*

III. Prelazne i završne odredbe

Član 43.

Stupanjem na snagu ovog Pravilnika, prestaje da važi Pravilnik o bezbednosti informaciono-komunikacionog sistema opštine Tutin br. IV-258/2020.

Član 44.

Ovaj pravilnik stupa na snagu danom objavljivanja na zvaničnoj internet prezentaciji Opštine Tutin. www.tutin.rs.

Načelnik opštinske uprave opštine Tutin

Muamer Mavrić

Republika Srbija
- Opština Tutin -
Opštinska
uprava
200084037

Digitally signed by
Republika Srbija -
Opština Tutin -
Opštinska uprava
200084037
Date: 2026.07.01
13:46:33 +02'00'

MUAMER
MAVRIĆ
012251220
Auth

Digitally signed
by MUAMER
MAVRIĆ
012251220 Auth
Date: 2026.07.01
13:47:01 +02'00'