

Na osnovu člana 8. stav 1. Zakona o informacionoj bezbednosti („Službeni glasnik RS”, broj 6/16), člana 2. Uredbe o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere informaciono-komunikacionih sistema od posebnog značaja i sadržaju izveštaja o proveri informaciono-komunikacionog sistema od posebnog značaja („Sl. glasnik RS“, br. 94/2016) i člana 37. Statuta Javnog preduzeća za prevoz putnika u gradskom i prigradskom saobraćaju „Subotica-trans“ Subotica br. 01/1-1205/2 od 08.05.2013. godine, dana 02.03.2017. godine, direktor preduzeća Aleksandar Aleksić, dipl. ekon. doneo je:

SUBOTICA-TRANS			
SUBOTICA			
Primljeno:		010317	
Op. jed.	Broj	Prilog	Vrednost
011	579/11		

**PRAVILNIK  
O BEZBEDNOSTI  
INFORMACIONO-KOMUNIKACIONOG SISTEMA  
JAVNOG PREDUZEĆA “SUBOTICA-TRANS” SUBOTICA**

## I Opšte odredbe

### Član 1.

Ovim Pravilnikom se, u skladu sa Zakonom o informacionoj bezbednosti i Uredbom o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere informaciono-komunikacionih sistema od posebnog značaja i sadržaju izveštaja o proveri informaciono-komunikacionog sistema od posebnog značaja, utvrđuju mere zaštite, principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti informaciono-komunikacionog sistema, (u daljem tekstu: IKT sistem), kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema Javnog preduzeća za prevoz putnika u gradskom i prigradskom saobraćaju “Subotica-trans” Subotica (u daljem tekstu: Operator).

### Član 2.

Informaciona dobra Operatora su svi resursi koji sadrže poslovne informacije Operatora, odnosno svi resursi 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 i sl.

O informacionim dobrima vodi se evidencija poslova na posebnom obrascu od strane Referenta informatike.

### Član 3.

Pod poslovima iz oblasti bezbednosti IKT sistema smatraju se:

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

## II Korišćenje IKT sistema

### Član 4.

IKT sistemom upravlja nadležni subjekt IKT sistema.

Nadležni subjekt IKT sistema je dužan da svakog novozaposlenog - korisnika IKT resursa upozna sa odgovornostima i pravilima korišćenja IKT resursa Operatora, da ga obuča za korišćenje resursa IKT sistema, da po završetku obuke od zaposlenog uzme izjavu o obučenosti za korišćenje IKT resursa i da o istima vodi evidenciju.

### Član 5.

U slučaju promene radnog mesta, odnosno nadležnosti korisnika - zaposlenog nadležni subjekt IKT sistema će izvršiti promenu prava u korišćenju IKT sistema koje korisnik -zaposleni imao u skladu sa opisom radnih zadataka.

### Član 6.

U slučaju prestanka radnog angažovanja korisnika - zaposlenog, korisnički nalog se ukida.

Korisnik IKT resursa, kome je prestalo radno angažovanje po bilo kom osnovu kod Operatora, ne sme da otkriva podatke koji su od značaja za informacionu bezbednost IKT sistema.

### *Administratorski i korisnički nalog*

### Član 7.

Pravo pristupa IKT sistemu imaju samo zaposleni, odnosno korisnici koji imaju administratorske i korisničke naloge

Administratorski nalog je jedinstven nalog kojim je omogućen pristup i administracija svih resursa IKT sistema, samo sa jednim korisničkim nalogom, kao i otvaranje novih i izmena postojećih naloga, može da koristi samo zaposleni koji je raspoređen na poslove i radne zadatke administratora..

Korisnički nalog je nalog koji sadrži korisničko ime i lozinku, koji se mogu ukucavati ili čitati sa medija na kome postoji elektronski sertifikat, na osnovu kojih se vrši autentifikacija – provera identiteta i autorizacija – provera prava pristupa, odnosno prava korišćenja resursa IKT sistema od strane zaposlenog - korisnika.

Korisnički nalog dodeljuje administrator, na osnovu zahteva zaposlenog zaduženog za upravljanje ljudskim resursima i to tek nakon unosa podataka o zaposlenom u softver za upravljanje ljudskim resursima. Na osnovu poslova i radnih zadataka zaposlenog, administrator određuje prava pristupa u skladu sa potrebama obavljanja poslovnih zadataka od strane zaposlenog-korisnika.

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

### *Odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju*

### Član 8.

Korisnički nalog se sastoji od korisničkog imena i lozinke.

Latinična slova koja se ne upotrebljavaju	Latinična slova koja se upotrebljavaju
đ	dj
ž	z
lj	lj
nj	nj
ć, č, š	c
dž	Dz

Lozinka mora da sadrži minimum sedam karaktera kombinovanih od malih i velikih slova i cifara.

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

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

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

### III Predmet, mere i subjekti zaštite IKT sistema

#### Član 9.

Predmet zaštite IKT sistema 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.

#### Član 10.

Mere propisane ovim aktom se odnose na sve organizacione jedinice IKT sistema Operatora, na sve zaposlene - korisnike informatičkih resursa, kao i na treća lica koja koriste informatičke resurse Operatora.

#### Član 11.

Merama zaštite IKT sistema Operatora obezbeđuje se 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.

Radi zaštite tajnosti, autentičnosti i integriteta podataka, Operator može da razmotri korišćenje odgovarajućih mera kriptozastite.

#### Član 12.

Za obavljanje poslova iz oblasti bezbednosti IKT sistema Operatora nadležan je Referent informatike.

### **Član 13.**

Zaposleni u Operateru je dužan da poštuje i sledeća pravila bezbednog i primerenog korišćenja resursa IKT sistema:

- 1) da koristi informatičke resurse isključivo u poslovne svrhe;
- 2) da prihvati da su svi podaci koji se skladište, prenose ili procesiraju u okviru informatičkih resursa vlasništvo Operatora i da mogu biti predmet nadgledanja i pregledanja;
- 3) da postupa sa poverljivim podacima u skladu sa propisima, a posebno prilikom kopiranja i prenosa podataka;
- 4) da bezbedno čuva svoje lozinke u odnosu na druga lica;
- 5) da menja lozinke saglasno utvrđenim pravilima;
- 6) da se, pre svakog udaljavanja od radne stanice, odjavi sa sistema, odnosno zaključa radnu stanicu;
- 7) da koristi DVDRW, CDRW i USB eksterne memorije na radnoj stanici samo uz odobrenje nadležnog subjekta IKT sistema;
- 8) da zahtev za instalaciju softvera ili hardvera podnosi u pisanoj formi, odobren od strane neposrednog rukovodioca;
- 9) da obezbedi sigurnost podataka u skladu sa važećim propisima;
- 10) da pristupa informatičkim resursima samo na osnovu izričito dodeljenih korisničkih prava od strane nadležnog subjekta;
- 11) da ne sme da zaustavlja rad ili briše antivirusni program, menja njegove podešene opcije, niti da neovlašćeno instalira drugi antivirusni program;
- 12) da ne sme da na radnoj stanici skladišti sadržaj koji ne služi u poslovne svrhe;
- 13) da izrađuje zaštitne kopije (backup) podataka u skladu sa propisanim procedurama;
- 14) da koristi Internet i Internet e-mail servis Operatora u skladu sa propisanim procedurama;
- 15) da prihvati da se određene vrste informatičkih intervencija obavljaju u utvrđeno vreme;
- 16) da prihvati da svi pristupi informatičkim resursima i informacijama treba da budu zasnovani na principu minimalne neophodnosti;
- 17) da prihvati instalaciju tehnika i programa u cilju sigurnosti IKT sistema.
- 18) da ne sme da instalira, modifikuje, isključuje iz rada ili briše zaštitni, sistemski ili aplikativni softver.

*Ograničenje pristupa podacima i sredstvima za obradu podataka*

### **Član 14.**

Pristup resursima IKT sistema određen je vrstom naloga koji zaposleni ima.

Zaposleni 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.

Zaposleni 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.

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

## **IV Pojedinačne mere zaštite**

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

### **Član 15.**

Prostor u kome se nalaze računari za vođenje baza podataka i centralni računar (server), mrežna ili komunikaciona oprema IKT sistema, organizuje se kao administrativna zona.

Administrativna zona se uspostavlja za fizički pristup resursima IKT sistema u kontrolisanom, vidljivo označenom prostoru, koji je obezbeđen mehaničkom bravom.

### **Član 16.**

Ulaz u prostoriju u kojoj se nalazi IKT oprema, dozvoljen je samo administratoru IKT sistema.

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 uprave.

Prostorija iz stava 1. ovog člana 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 mediji sa podacima.

Prozori i vrata na ovoj prostoriji iz stava 1. ovog člana moraju uvek biti zatvoreni.

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, automatski se isključuje oprema.

U slučaju iznošenja opreme iz prostorije iz stava 1. ovog člana radi selidbe, ili servisiranja, neophodno je odobrenje neposrednog rukovodioca koji će odrediti uslove, način i mesto iznošenja opreme.

Ako se oprema iznosi radi servisiranja, pored odobrenja neposrednog rukovodioca, potrebno je sačiniti zapisnik u kome se navodi naziv i tip opreme, serijski broj, naziv servisera, ime i prezime ovlašćenog lica servisera.

Ugovorom sa serviserom obavezno se definiše obaveza zaštite podataka koji se nalaze na medijima koji su deo IKT resursa Operatera.

*Bezbednost rada na daljinu i upotreba mobilnih uređaja*

### **Član 17.**

Pristup resursima IKT sistema Operatora neregistrovanim korisnicima, putem mobilnih uređaja, omogućen je samo web site-u.

Zaposleni korisnici resursa IKT sistema, mogu putem mobilnih uređaja, koji su u vlasništvu Operatera i koji su podešeni od strane nadležnog subjekta u IKT sistemu, da pristupaju samo onim delovima IKT sistema koji im omogućavaju obavljanje radnih zadataka u okviru njihove nadležnosti kao što su elektronska pošta, pojedine aplikacije vezane za obavljanje posla i drugo, a na osnovu pisane saglasnosti neposrednog rukovodioca.

Mobilni uređaji moraju biti podešeni tako da omoguće siguran i bezbedan pristup, korišćenjem VPN mreže IKT sistema i liste MAC adresa uređaja putem kojih je dozvoljen pristup, uz aktivan odgovarajući softver za zaštitu od virusa i drugog zlonamernog softvera.

Zaposlenom je zabranjena je samostalna instalacija softvera i podešavanje mobilnog uređaja, kao i davanje uređaja neovlašćenim licima.

Zaposlenom je zabranjena je samostalna instalacija softvera i podešavanje mobilnog uređaja, kao i davanje uređaja neovlašćenim licima.

Nadležni subjekt u IKT sistemu svakodnevno kontroliše pristup resursima IKT sistema i proverava da li ima pristupa sa nepoznatih uređaja, odnosno nepoznatih MAC adresa.

Ukoliko se ustanovi neovlašćen pristup o tome se putem elektronske pošte odmah, a najkasnije sutradan obaveštava načelnik uprave, a te MAC adresa se unosi u blok listu softvera koji se koristi za kontrolu pristupa.

#### **Član 18.**

Pristup resursima IKT sistema sa privatnog uređaja nije dozvoljen, osim ako je uređaj u vlasništvu Operatera oštećen i nije obezbeđena zamena.

Saglasnost na korišćenje privatnog uređaja u slučaju iz stava 1. ovog člana daje neposrednog rukovodioca.

Evidenciju privatnih uređaja sa kojih će biti omogućen pristup vodi nadležni subjekt IKT sistema.

#### **Član 19.**

Privatni uređaji sa kojih će se pristupati resursima IKT sistema moraju biti podešeni od strane nadležnog subjekta IKT sistema.

Privatni uređaji sa kojih se može pristupati resursima IKT sistema mogu se koristiti samo za obavljanje poslova u nadležnosti korisnika - zaposlenog i to samo u periodu kada nije moguće koristiti uređaj u vlasništvu Operatera.

Nadležni subjekt IKT sistema je dužan da pre predaje uređaja ovlašćenom servisu, uradi backup podataka koji se nalaze u mobilnom uređaju.

#### *Zaštita nosača podataka*

#### **Član 20.**

Podaci koji se nalaze u IKT sistemu predstavljaju tajnu u skladu sa odredbama Zakona o slobodnom pristupu informacijama od javnog značaja, Zakona o zaštiti podataka o ličnosti, Zakona o tajnosti podataka, kao i Uredbe o načinu i postupku označavanja tajnosti podataka, odnosno dokumenata.

Podaci koji se označe kao tajni, moraju biti zaštićeni u skladu sa odredbama Uredbe o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima.

#### **Član 21.**

Nadležni subjekt u IKT sistemu će uspostaviti organizaciju pristupa podacima, posebno onima koji budu označeni tajnim u skladu sa Zakonom o tajnosti podataka, tako da dokumenti sa oznakom tajnosti mogu da se snime, odnosno arhiviraju ili zapišu na fajl serveru u folderu nad kojim će pravo pristupa imati samo zaposleni - korisnici koji na to budu imali pravo.

Dokumenti sa oznakom tajnosti mogu da se snime na druge nosače (eksterni HDD, USB, CD, DVD) samo od strane neposrednog rukovodioca ili njegovim pisanim aktom ovlašćenih zaposlenih – korisnika.

Evidenciju nosača na kojima su snimljeni podaci sa oznakom tajnosti, vodi nadležni subjekt IKT sistema.

Nosači na kojima se nalaze dokumenti sa oznakom tajnosti moraju biti propisno obeleženi i odloženi na mesto na kome će biti zaštićeni od neovlašćenog pristupa.

Prilikom brisanja podataka za oznakom tajnosti sa nosača na kojima su se nalazili, podaci moraju biti nepovratno obrisani, a ako to nije moguće, takvi nosači moraju biti fizički oštećeni, odnosno uništeni.

#### *Obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka*

##### **Član 22.**

Za razvoj i testiranje softvera pre uvođenja u rad u IKT sistem moraju se koristiti serveri koji su namenjeni testiranju i razvoju. Zabranjeno je korišćenje servera koji se koriste u operativnom radu za testiranje softvera.

Pre uvođenja u rad novog softvera neophodno je napraviti kopiju - arhivu postojećih podataka.

Instaliranje novog softvera kao i ažuriranje postojećeg, odnosno instalacija nove verzije vrši se po završetku radnog vremena, kako ne bi bio zaustavljen operativni rad zaposlenih - korisnika.

#### *Zaštita podataka i sredstva za obradu podataka od zlonamernog softvera*

##### **Član 23.**

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, e-mailom, zaraženim prenosnim medijima (USB memorija, CD i td.), instalacijom nelicenciranog softvera i sl.

Za uspešnu zaštitu od virusa na svakom računaru se instalira antivirusni program.

Svakodnevno se automatski vrši dopuna antivirusnih definicija.

Antivirusni program u kontinuitetu kontroliše računare u realnom vremenu.

#### *Zaštita pri korišćenju interneta*

##### **Član 24.**

U cilju zaštite, odnosno upada u IKT sistem Operatera sa interneta, nadležni subjekt IKT sistema je dužan da održava sistem za sprečavanje upada putem Firewall i Routera.

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

Funkcioneri i zaposleni kojima je odobreno korišćenje interneta i elektronske pošte dužni su da prilikom korišćenja istog postupaju po međunarodnim konvencijama i pravilima ponašanja.

Korisnicima koji su priključeni na IKT sistem je zabranjeno samostalno priključenje na internet, odnosno priključenje preko sopstvenog modema.

Nadležni subjekt IKT sistema može ukinuti pristup internetu u slučaju dokazane zloupotrebe istog.

Korisnici IKT sistema kojima je odobreno korišćenje interneta dužni su da se pridržavaju mera zaštite od virusa i upada sa interneta u IKT sistem, a svaki računar čiji se zaposleni - korisnik priključuje na Internet mora biti odgovarajuće podešen i zaštićen, pri čemu podešavanje vrši nadležni subjekt IKT sistema.

Prilikom korišćenja interneta korisnik IKT sistema kome je odobreno korišćenje interneta dužan je izbegavati sumnjive WEB stranice, u cilju sprečavanja instaliranja programa koji mogu naneti štetu IKT sistemu.

Prilikom korišćenja interneta korisnik IKT sistema kome je odobreno korišćenje interneta dužan je izbegavati sumnjive WEB stranice, u cilju sprečavanja instaliranja programa koji mogu naneti štetu IKT sistemu.

U slučaju da korisnik primeti neobično ponašanje računara, tu pojavu je dužan da bez odlaganja prijavi nadležnom subjektu IKT sistema.

#### **Član 25.**

Korisniku IKT sistema kome je dozvoljeno korišćenje interneta zabranjeno je gledanje filmova i igranje igrice na računarima i pretraživanje WEB stranica koje sadrže pornografski i ostali nedoličan sadržaj, kao i samovoljno preuzimanje istih sa interneta.

#### **Član 26.**

Nedozvoljena upotreba interneta obuhvata i:

- 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 druga vrsta nedozvoljenih softvera);
- nedozvoljeno korišćenje društvenih mreža i drugih internet sadržaja koje je ograničeno odlukom nadležnog organa Operatora;
- preuzimanje podataka u količini koja prouzrokuje veliko opterećenje na mreži;
- preuzimanje materijala zaštićenih autorskim pravima;
- korišćenje linkova koji nisu u vezi sa poslom;
- nedozvoljeni pristup sadržaju, promena sadržaja, brisanje ili prerada sadržaja preko interneta.

#### *Zaštita od gubitka podataka*

#### **Član 27.**

Baze podataka obavezno se arhiviraju na back-up server, najmanje jednom dnevno, nedeljno, mesečno i godišnje, za potrebe obnove baze podataka.

Ostali fajlovi - dokumenti se arhiviraju najmanje jednom nedeljno, mesečno i godišnje.

Podaci o zaposlenima - korisnicima, arhiviraju se najmanje jednom mesečno.

#### **Član 28.**

Dnevno kopiranje - arhiviranje vrši se za svaki radni dan u sedmici, od 23:00 časova svakog radnog dana i na Autobuskoj stanici i u sedištu Operatera.

Nedeljno kopiranje - arhiviranje vrši se poslednjeg radnog dana u nedelji, od 23:00 časova, u onoliko nedeljnih primeraka koliko ima poslednjih radnih dana u mesecu.

Mesečno kopiranje - arhiviranje vrši se poslednjeg radnog dana u mesecu, za svaki mesec posebno, od 23:00 časova.

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

#### **Član 29.**

Svaki primerak godišnje kopije - arhive čuva se u roku od godinu dana.

Dnevne, nedeljne i mesečne kopije - arhive se čuvaju u prostoriji koja je fizički i u skladu sa merama zaštite od požara obezbeđena.

### **Član 30.**

Ispravnost kopija - arhiva proverava se najmanje na šest meseci i to tako što se vrši vraćanje baza podataka koje se nalaze na mediju, pri čemu podaci posle vraćanja treba da budu ispravni i spremni za upotrebu.

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

### **Član 31.**

O aktivnostima administratora i zaposlenih - korisnika vodi se dnevnik aktivnosti (log).

Svakog poslednjeg radnog dana u nedelji datoteka u kojoj se nalazi dnevnik aktivnosti se arhivira po proceduri za izradu kopija - arhiva ostalih podataka i IKT sistemu, u skladu sa čl. 27. ovog Pravilnika.

*Sistem za kontrolu*

### **Član 32.**

Sistem za kontrolu i dojavu o greškama, neovlašćenim aktivnostima i drugim mogućim problemima u IKT sistemu, mora biti podešen tako da odmah obaveštava nadležnog subjekta IKT sistema o svim neregularnim aktivnostima zaposlenih - korisnika, pokušajima upada i upadima u sistem.

*Obezbeđivanje integriteta softvera i operativnih sistema*

### **Član 33.**

U IKT sistemu može da se instalira samo softver za koji postoji važeća licenca u vlasništvu Operatora, odnosno Freeware i Open source verzije.

Instalaciju i podešavanje softvera može da vrši samo nadležni subjekt IKT sistema, odnosno zaposleni - korisnik koji ima ovlašćenje za to.

Instalaciju i podešavanje softvera može da izvrši i treće lice, u slučaju da je softver nabavljen u postupku javne nabavke, a na način definisan sa Ugovorom o nabavci.

Treće lice može da izvrši Instalaciju i podešavanje softvera kada je između Operatora i njega ugovoreno održavanje softvera u određenom vremenskom periodu.

### **Član 34.**

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.

*Zaštita od zloupotrebe bezbednosnih slabosti IKT sistema*

### **Član 35.**

Nadležni subjekt IKT sistema najmanje jednom mesečno, a po potrebi i češće vrši analizu dnevnika aktivnosti (loga) u cilju identifikacije potencijalnih slabosti IKT sistema.

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

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

#### *Reviziji IKT sistema*

##### **Član 36.**

Revizija IKT sistema se mora vršiti tako da ne ometa poslovne procese korisnika-zaposlenih.

Nadležni subjekt IKT sistema određuje vreme obavljanja revizije, u zavisnosti od vrste poslova i radnih zadataka zaposlenih – korisnika u Operatoru.

#### *Zaštita opreme IKT sistema*

##### **Član 37.**

Komunikacioni kablovi i kablovi za napanje moraju biti postavljeni u zid ili kanalnice, tako da se onemoguću neovlašćen pristup, odnosno da se izvrši izolacija.

Mrežna oprema (switch, router, firewall) moraju se nalaziti u rack ormanu, zaključani.

Nadležni subjekt IKT 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 posetioci objekata, mora biti odvojena od interne mreže koju koriste korisnici zaposleni i kroz koju se vrši razmena službenih podataka. Ta mreža treba da bude označena (SSID).

#### *Bezbednost IKT sistema u slučaju razmene podataka*

##### **Član 38.**

Razmena podataka koji su označeni oznakom tajnosti sa drugim organima, organizacijama ili pravni licima se vrši u skladu sa potpisanim aktom o razmeni podataka.

Akt iz stava 1. ovog člana sadrži podatke o ovlašćenim licima za razmenu podataka, načinu razmene podataka, pravni okvir za takvu vrstu razmene, kao i pravni okvir kojim se definiše zaštita podataka koji se razmenjuju.

#### *Zaštita podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova sistema*

##### **Član 39.**

Za potrebe testiranja IKT sistema, odnosno delova sistema nadležni subjekt IKT sistema može da koristi podatke koji nisu označeni oznakom tajnosti, odnosno službenosti.

#### *Učešće trećih lica u poslovima IKT sistema*

##### **Član 40.**

Način instaliranja novih, zamena i održavanje postojećih resursa IKT sistema od strane trećih lica koja nisu zaposlena kod Operatora, reguliše se međusobno zaključenim ugovorom.

Nadležni subjekt IKT sistema je zadužen za tehnički nadzor nad realizacijom ugovorenih obaveza od strane trećih lica.

#### **Član 41.**

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.

Nadležni subjekt IKT sistema je odgovoran za kontrolu pristupa i nadzor nad izvršenjem ugovorenih obaveza, kao i za poštovanje odredbi ovog Pravilnika kojima su takve aktivnosti definisane.

#### **Član 42.**

Nadležni subjekt IKT sistema 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 nadležni subjekt IKT sistema je dužan da odmah obavesti neposrednog rukovodioca, radi preduzimanja mera u cilju otklanjanja nepravilnosti.

*Preventivne mere i reagovanje na bezbednosne incidente*

#### **Član 43.**

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

Po prijemu prijave stava 1. ovog člana nadležni subjekt IKT sistema je dužan da odmah obavesti neposrednog rukovodioca i preduzme mere u cilju zaštite resursa IKT sistema.

#### **Član 44.**

Ukoliko se radi o incidentu koji je definisan u Uredbom o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja, nadležni subjekt IKT je dužan da pored neposrednog rukovodioca obavesti i direktora preduzeća.

Nadležni subjekt IKT 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.

### **V Izmene postojećeg i uspostavljanje novog IKT sistema**

#### **Član 45.**

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

Dokumentacija iz stava 1. ovog člana mora da sadrži opise svih procedura a posebno procedura koje se odnose na bezbednost IKT sistema.

### **VI Mere u cilju obezbeđenja kontinuiteta obavljanja posla u vanrednim okolnostima**

#### **Član 46.**

U slučaju vanrednih okolnosti, koje mogu da dovedu do izmeštanja IKT sistema iz zgrade uprave, nadležni subjekt IKT 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 nadležni subjekt IKT sistema, u tri primerka, od kojih se jedan nalazi kod njega, drugi kod zaposlenog nadležnog za poslove odbrane i vanredne situacije, a treći primerak kod neposrednog rukovodioca.

Delove IKT sistema koji nisu neophodni za funkcionisanje u vanrednim situacijama, skladište se na rezervnu lokaciju, koju odredi neposredni rukovodilac.

Skladištenje delova IKT sistema koji nisu neophodni vrši se na način da oprema bude bezbedna i obeležena, u skladu sa evidencijom koja se o njoj vodi.

## VII Provera IKT sistema

### Član 47.

Proveru IKT sistema vrši nadležni subjekt IKT sistema.

### Član 48.

Provera će se vršiti poslednjeg meseca u godini.

### Član 49.

Provera IKT sistema se vrši tako što se:

- 1) proverava usklađenost Pravilnika o bezbednosti IKT sistema, uzimajući u obzir i akta na koji 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 neposrednom rukovodiocu..

### Član 50.

Izveštaj iz člana 49. ovog Pravilnika sadrži:

- 1) naziv Operatora;
- 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.

