ПОЖАРЕВАЦ
ВОДОВОД
и канализација

JKP „Vodovod i kanalizacija" Požarevac, Dr. *Voje Dulića 4, Požarevac*, tel. 012/555-801, email. office@vodovod012.rs

Na osnovu člana 42. Statuta JKP „Vodovod i kanalizacija" Požarevac број 01-6492/1 od 14.12.2016. godine direktor donosi

PRAVILNIK O UPOTREBI RAČUNARA I INFORMACIONOG SISTEMA JKP "VODOVDO I KANALIZACIJA" POŽAREVAC

1. OPŠTE ODREDBE

Član 1.

Pravilnikom o upotrebi računara i informacionog sistema JKP "Vodovod i kanalizacija" Požarevac (u daljem tekstu: Pravilnik) uređuje se struktura informacione tehnologije JKP „Vodovod i kanalizacija" Požarevac, upotreba računarske opreme i informacionog sistema od strane zaposlenih u JKP „Vodovod i kanalizacija" Požarevac, postupak dodele, upotrebe i ukidanje korisničkog naloga zaposlenih u JKP „Vodovod i kanalizacija" Požarevac, pravila o bezbednosti i zaštiti korišćenja podataka i infrastrukture informaciono-komunikacionog sistema i druga pitanja značajna za pravilnu upotrebu informacionog sistema.

2. INFORMACIONI SISTEM JKP "VODOVOD I KANALIZACIJA" POŽAREVAC

Član 2.

Informacioni sistem JKP "Vodovod i kanalizacija" Požarevac sastoji se od niza korisničkih umreženih računara, koje koriste zaposleni JKP "Vodovodi kanalizacija" Požarevac povezanih jedinstvenom mrežom sa dva servera. Mreža i svaki korisnički računar poseduju izlaz ka internetu dok su serveri na mreži zatvoreni od izlaska na internet kako bi podaci bili zaštićeni od eksternih pristupa.

Član 3.

JKP "Vodovod i kanalizacija" Požarevac (u daljem tekstu: Preduzeće) poseduje dva servera i to server naplate i server računovodstva.

Server naplate je server sa operativnim sistemom Microsoft Windows server 2003 sa softverskim paketom OMNI DATA Šabac program Naplate. Server ima svoju jedinstvenu IP adresu dodeljenu za raspoznavanje na mreži.

Programski paket Naplate kontroliše i radi putem Access programa Microsoft Office 2003. Jedinstvena baza programskog paketa je u MDB formatu i u sebi od podataka sadrži jedinstvene matične brojeve, imena i prezimena kao i ulice stanovanja potrošača, korisničke ugovore, brojeve vodomera, sve segmente privrede sa podacima o kupcu,

gde se može naći više potrošača, kućne savete sa podacima o mernom mestu i podacima o vodomeru. Od podataka tu se još nalaze ID (identifikacioni br - šifra) korisnika, podaci o uslugama koje koje koristi (usluge vode i kanalizacije) i kojoj kategoriji pripadaju.

Član 4.

Svaki korisnički računar koji zaposleni koristi a ima pristup serveru Naplate ima svoje jedinstveno korisničko ime kao i šifru koji sadrže velika i mala slova, brojeve i znakove. Dužina šifre ne može biti kraća od 6 karaktera, a najduža je 16.

Član 5.

Pristup serveru se omogućava preko RDP-a (remote desktop pristup).

Korisnik se dodeljuje po nalogu rukovodioca kome se potom otvara nalog na serveru od strane administratora, a potom se otvara korisnik u programu Naplata koji takođe sadrži jedinstveno korisničko ime kao i šifru koje sadrže velika i mala slova, brojeve i znakove. Dužina šifre ne može biti kraća od 6 karaktera a najduža je 16.

Član 6.

Baza programskog paketa Naplata ima već predodređen sistem pravljenja kopija (backup) u samom programskom paketu. Svaka izrada rezervne kopije obavlja se automatski svakog dana u 11h i posle detaljne provere ispravnosti izrađene rezervne kopije skladišti na određenom tvrdom disku (hard disk) izdvojenom od pristupa čitanja programskog paketa i dalje modifikacije i promene.

Ukoliko dođe do potrebe za povratkom podataka (ukoliko je došlo do kvara na određenom segmentu tvrdog diska koji pokriva deo glavne baze povratak (restore) se vrši iz tog izolovanog dela raspakivanjem a potop kopiranjem rezervne kopije u glavni operativni folder namenjen glavnoj operativnoj bazi podataka.

Celu proceduru izrade rezervne kopije baze podataka kao i povraćaj rezervne kopije radi administrator baze podataka programskog paketa Naplata.

Član 7.

Server računovodstva kontroliše operativni sistem Microsoft Windows server 2012. Server ima svoju jedinstvenu IP adresu dodeljenu za raspoznavanje na mreži.

Programski paket računovodstva koji se na serveru koristi je programski paket proizvođača DataLab a program Pantheon. Server ne poseduje Microsoft Office paket jer se u programskom paketu koji se koristi već nalaze formati doc, xls kao i PDF za obradu tj. export podataka.

Zbog količine i kompleksnosti podataka koji se obrađuju i način funkcionisanja softvera koristi se Microsoft SQL server, a kako se ne koristi količina podataka u meri od preko veličine 10Gb veličine fajla koristi se besplatno rešenje Microsoft SQL server

Express. Baza se nalazi u formatu sql. Za pristup programskom paketu koristi se P2P (peer to peer) pristup.

Član 8.

Instaliran program za pristup bazi koja se nalazi na serveru nalazi se na korisničkom računaru te se ikonicom sa desktop-a klijentskog računara i podešenim parametrima pristupa programskom paketu.

Korisnik programskog paketa nema pristup serveru računovodstva ni u jednom drugom obliku osim navedenim pristupom samom programu u stavu 1. ovog člana i preko njegovog korisničkog interfejsa bazi računovodstva.

Izrada rezervne kopije baze računovodstva izrađuje automatski Microsoft SQL server Express sa poslom (Job) zadatim za izrađivanje rezervne kopije svakog dana po završetku radnog vremena. Svaka rezervna kopija skladišti se na odvojenom tvrdom disku (hard disk) zapakuje u rar formatu i odvaja za čuvanje u slučaju nastanka problema rada glavne baze i drugih vidova oštećenja.

Povraćaj podataka radi administrator preko Microsoft SQL server Express implementiranom funkcijom povraćaja (restore) u samom Microsoft SQL server Express.

Član 9.

Od podataka u bazi programskog paketa DataLab Pantheon nalaze se fizička lica sa imenom prezimenom, jedinstvenim matičnim brojem i adresom stanovanja. Pravna lica sa nazivom firme, sedištem, PIB-om, matičnim brojem, ugovori, računi, predračuni.

Član 10.

U delu baze programskog paketa DataLab Pantheon nalaze se podaci o zaposlenima i to:

1. Ime prezime srednje ime;
2. JMBG;
3. Adresa stanovanja
4. Datum zaposlenja
5. Doneti radni staž
6. Radno mesto
7. Služba
8. Procenat minulog rada
9. Koeficijent za obračun zarade
10. Sve podatke o obračunima koji su obračunati radniku (zarade, bolovanja, prevoz, jubilarne nagrade, dnevnice....)
11. Broj tekućeg računa
12. Sindikat

13. Administrativne zabrane

Član 11.

U drugom delu pogramskog paketa DataLab Panteon nalaze se računovodstveni podaci i to o:

Kupcima fizičkim licima:
- šifra kupca
- ime i prezime
- adresa i mesto prebivališta
- podaci na konto karticama o izdatim računima, avansnim računima i uplatama sa datumima evidentiranja poslovnih promena.

Kupcima pravnim licima:
- šifra kupca
- naziv pravnog lica
- adresa i sedište
- PIB i matični broj pravnog lica
- kontakt telefon i faks (podatak postoji samo za određene kupce)
- podaci na konto karticama o izdatim računima, avansnim računima i uplatama sa datumima evidentiranja poslovnih promena.

Član 12.

Serveri Preduzeća nalaze se u odvojenoj prostoriji sa izolovanim pristupom. Povezani su sa nizom switch uređaja putem patch panela, na kome se nalazi obeležje izlaza, brojem izlaza, kojim se definiše elektronski pristup STP kablovima samim prostorijama u kojima se nalaze zaposleni. Zaposleni radi pristupa imaju fiksnu IP adresu iz opsega dodeljenog, radi prepoznavanja na mreži i limitiranog i praćenog pristupa IT infrastrukturi Preduzeća.

3. UPOTREBA RAČUNARSKE OPREME I INFORMACIONOG SISTEMA

3.1 Postupak pojedinačnog priključivanja i lokalnog organizovanja računara

Član 13.

Pojedinačno priključivanje korisničkog računara na računarsku mrežu Preduzeća ne sme ničim da ugrozi fizički i logički integritet informaciono-kominikacionog sistema Preduzeća.

JKP „Vodovod i kanalizacija“ Požarevac, Dr. Voje Dulića 4, Požarevac, tel. 012/555-801, email. office@vodovod012.rs

Računar priključen na računarsku mrežu Preduzeća, zajedno sa instaliranim operativnim sistemom, smatra se fizičkim i logičkim delom informaciono-komunikacionog sistema Preduzeća.

Samo računar koji je registrovan od ovlašćenog zaposlenog (u daljem tekstu: administrator preduzeća) može da bude priključen na računarsku mrežu Preduzeća. Od ovog se izuzimaju prenosni računari.

Član 14.

Pojedinačno priključivanje korisničkog računara se isključivo sprovodi prema proceduri:

1. Podnošenje zahteva za priključivanje računara na računarsku mrežu informacionog-komunikacionog sistema Preduzeća,

2. Odluku o priključivanju računara na računarsku mrežu informacionog-komunikacionog sistema Preduzeća donosi direktor izdavanjem pisanog naloga za priključivanje administratoru preduzeća,

3. Priključivanje računara na računarsku mrežu iformacionog-komunikacionog sistema Preduzeća obavlja administrator preduzeća.

Član 15.

Postupak priključivanja obuhvata sledeće aktivnosti:

- Provera funkcionalnosti i autorizacije operativnog sistema
- Provera funkcionalnosti i konfigurisanje mrežne kartice
- Priključivalje na komunikacioni kabl koji obezbeđuje Preduzeće
- Instalacija i konfigurisanje komunikacionih protokola
- Dodeljivanje adrese
- Instalacija i konfigurisanje softvera za pristup servisu elektronske pošte
- Instalacija antivirus programa
- Provera pristupa mreži, pristup servisu elektronske pošte, pristupa ostalim korisničkim servisima i posebna provera bezbednosnih aspekata
- Registracija računara

Član 16.

Priključno mesto je deo mrežnog razvoda informacionog - komunikacionog sitema Preduzeća.
Fizička instalacija novog priključnog mesta je isključivo u nadležnosti administratora preduzeća i može se izvesti samo uz njegovu saglasnost, a na osonovu pismenog odobrenja direktora.

Kada se instalacija novog priključnog mesta sprovodi po posebnom zahtevu onda se ona sprovodi na sledeći način:

1. Podnošenje pismenog zahteva za instalaciju novog priključnog mesta računarske mreže informacionog - komunikacionog sistema Preduzeća.
2. Odluku o instalaciji novog priključnog metsa informacionog - komunikacionog sistema Preduzeća donosi direktor.
3. Instalaciju novog priključnog mesta računarske mreže informacionog - komunikacionog sistema Preduzeća obavlja isključivo administrator preduzeća.

Član 17.

Prenosni računar se može priključiti na računarsku mrežu Preduzeća samo u kontekstu zamene stacionarnog računara koji je registrovan i priključen na mrežu i to tako što će se stacionarni računar isključiti a na njegovo mesto uključiti prenosni.

Korisnik prenosnog računara je dužan da instalira i podesi sve mrežne protokole i njihove parametre na istovetan način na koji je to bilo izvedeno na stacionarnom računaru.

U slučaju priključivanja prenosnog računara na neko drugo priključno mesto razvoda informacionog - komunikacionog sistema Preduzeća, stacionarni računar čija se zamena vrši mora da bude isključen kako bi se sprečilo dupliranje adresa.

Bežični pristup računarskoj mreži informacionog - komunikacionog Sistema Preduzeća, u formalnom i tehničkom smislu je ekvivalentan pristupu preko žičnog razvoda, i po tom osnovu u potpunosti postoji obaveza primene procedura.

Član 18.

Logička adresa, u bilo kom obliku, je zajednički resurs Preduzeća i njeno korišćenje dozvoljeno je isključivo u kontekstu poslovnih aktivnosti Preduzeća.

Dodeljivanje logičke adrese je u isključivoj nadležnosti administratora preduzeća, uz prethodno odobrenje direktora.

Član 19.

Neovlašćeno korišćenje logičke adrese ili njeno ustupanje drugom korisniku, smatra se najtežim oblikom kršenja pravila korektnog korišćenja mrežnih resursa informacionog-komunikacionog sistema Preduzeća.

Zaposleni kao korisnik priključenog računara (u daljem tekstu: korisnik računara) je odgovoran za bezbednost i integritet podataka koji se nalaze na računaru priključenom na računarsku mrežu Preduzeća.

U cilju zaštite od neovlašćenog pristupa računaru priključenom na računarsku mrežu Preduzeća obavezna je zaštita računara odgovarajućom lozinkom i antivirusnim programom koji se redovno ažurira.

Rad bez lozinke i antivirus programa, smatra se kršenjem pravila korektnog korišćenja mrežnih resursa informacionog-komunikacionog sistema Preduzeća.

Član 20.

Dodela prava pristupa internim resursima računara i mreže od strane korisnika računara za ostale zaposlene je u isključivoj nadležnosti korisnika računara. U tom kontekstu, administrator preduzeća ne snosi nikakvu odgovornost u slučaju bilo kog oblika neovlašćenog pristupa podacima ili oštećenja njihovog integriteta.

Član 21.

Svaki pojedinačan računar koji je priključen na računarsku mrežu Preduzeća mora da poseduje legalan operativan sistem. Korisnik računara po svom nahođenju bira operativni sistem. Instaliran korisnički softver nije obuhvaćen ovim pravilnikom i u isključivoj je nadležnosti korisnika računara.

Član 22.

Kad se iz tehničkih (zastarelost ili veliko oštećenje) ili nekih drugih razloga pojedinačno priključeni računar trajno isključuje sa mreže, korisnik računara je dužan da o tome pismeno obavesti administratora preduzeća.

Kod neposredne zamene starog računara novim, primenjuju se postupak ponovnog priključivanja.

U slučaju ponovnog instaliranja operativnog sistema ili bilo koje druge intervencije na računaru koja je u vezi sa podešavanjima komunikacionih protokola, uključujući i promenu mrežnog adaptera, postoji obeveza korisnika računara da o tome obavesti administratora preduzeća i da se od strane administratora preduzeća sprovede skraćena procedura priključivanja.

3.1.2 Lokalno organizovanje

Član 23.

Lokalno umrežavanje računara koji se preko svog servera priključuju na informaciono- kominukacioni sistem Preduzeća, smatra se proširenjem postojeće mreže Preduzeća i njenim novim segmentiranjem.

Lokalna mreža ne sme ničim da ugrozi fizički i logički integritet informacionog-komunikacionog sistema.

Računar priključen na računarsku mrežu Preduzeća, kome je dodeljena adresa iz javnog adresnog domena i na kome je instaliran neki od javnih servisa, dobija status servera lokalne mreže.

JKP „Vodovod i kanalizacija“ Požarevac, Dr. Voje Dulića 4, Požarevac, tel. 012/555-801, email. office@vodovod012.rs

Samo registrovane lokalne mreže koje zadovoljavaju uslove, mogu da budu priključene na informaciono-kominikacioni sistem Preduzeća.

Računari povezani u lokalnu mrežu ne mogu da koriste javni adresni prostor i ne moraju da budu registrovani od strane Preduzeća .

Lokalno umrežavanje računara, dozvoljeno je samo na nivou oragnizacionih jedinica Preduzeća i može da se koristi isključivo u kontekstu poslovnih aktivnosti Preduzeća.

Član 24.

Lokalne mreže zajedničkih službi Preduzeća su u isključivoj nadležnosti administratora preduzeća, uključujući administraciju servera-mreže i njeno tehničko održavanje.

Lokalno umrežavanje može se dozvoliti samo uz pisanu saglasnost administratora preduzeća i pisano odobrenje direktora, pri čemu se sprovodi sledeća procedura:

- Podnošenje pisanog zahteva rukovodioca organizacione jedinice u kome se navodi precizan tehnički opis. U formulisanju zahteva može se konsultovati administrator preduzeća ili se kompletan postupak može prepustiti u tehničkom smislu administrator preduzeća (skraćena procedura),
- Zahtev razmatra administrator preduzeća i na osnovu dostavljenih podataka i tehničkih uslova daje predlog za odobravanje formiranja lokalne mreže pisani predlog prosleđuje direktoru.

Administeator preduzeća po okončanju svih tehničkih aktivnosti i stavljanje lokalne mreže u funkciju, pisanim putem obaveštava direktora Preduzeća.

Član 25.

Lokalna mreža mora da ima svog adminstratora, koji se smatra odgovrnim licem. Administrator lokalne mreže ima sledeće obaveze:

1. Neprekidno praćenje rada lokalne mreže,
2. Poštovanje uslova pod kojima je dozvoljeno lokalno umrežavanje, posebno u delu funkcije osnovnih mrežnih servisa,
3. Mora da obezbedi kontrolisani pristup svim lokalnim mrežnim resursima i odgovarajući antivirusnu zaštitu
4. zaposleni ovlašćen od strane direktora obavlja funkciju administratora preduzeća.

Član 26.

Administrator preduzeća ima obavezu evidencije pojedinačno priključenih računara na računarsku mrežu Preduzeća. Registraciju pojedinačno priključenog računara je obavezna.

Administrator preduzeća ima obavezu evidencije servera lokalnih mreža priključenih na računarsku mrežu Preduzeća. Registracija servera podrazumeva sledeće aktivnosti:

1. Identifikacija relevantnih sistemskih podataka servera i operativnog sistema
2. Identifikaciju licence instaliranog operativnog Sistema,
3. Dodeljivanje jedinstvenog identifikaciong broja,
4. Evidencija broja lokalno umreženih računara,
5. Identifikacija instaliranih javnih mrežnih servisa (namena lokalne mreže).

Administrator preduzeća ima ekskluzivno pravo da bez prethodne saglasnosti direktora privremeno ukine mogućnost pristupa pojedinačnog računara ili lokalne mreže, ukoliko proceni da je to u interesu bezbednosti komunikaciono-informativnog sistema Preduzeća.

Administrator preduzeća ima obavezu da ukine mogućnost pristupa računarskoj mreži Preduzeća svakom neregistrovanom računaru.

3.2 Postupak dodele, upotrebe i ukidanje korisničkih naloga

3.2.1 Dodeljivanje korisničkih naloga

Član 27.

Korisnički nalog je instrument koji omogućava legalni pristup mrežnim serverima informaciono-komunikacionog sistema Preduzeća. Zaposleni i druga lica angažovana po različitim ugovorima od strane Preduzeća koji su korisnici računara imaju parvo pristupa mrežnim serverima informaciono-komunikacionog Sistema Preduzeća.

Korisnici računara pored prava imaju i obavezu pristupa delu elektronske pošte.

Korisnički nalog dodeljuje administrator preduzeća na osnovu pisanog zahteva korisnika računara i pisane saglasnosti direktora.
Nosilac korisničkog naloga može da bude fizičko lice, funkcija ili služba.

3.2.2 Upotreba korisničkih naloga

Član 28.

Korisnički nalog je neotuđiv i isključivo ga može upotrebljavati samo nosilac naloga.
Korisniničko ime naloga je definisano: ime.prezime@vodovod012.rs
Odgovornost za upotrebu korisničkog naloga i njegovu privatnost (tajnost šifre) isključivo ima nosioc naloga. Kada je nosioc korisničkog naloga funkcija ili služba, onda se potpuna odgovornost vezuje za fizičko lice koje je nosilac funkcije ili rukovodioca službe.

Član 29.

Nosilac korisničkog naloga je isključivo odgovoran za poštovanje pravila korišćenja informaciono-komunikacionih resursa Preduzeća. Pored poštovanja opštih pravila rada na Internetu, obavezno je poštovanje i sledećeg:

1. Nosiocu korisničkog naloga nije dozvoljeno instaliranje i-ili podešavanje parametara mrežnih protokola uključujući IP adresu lokalnog računara kojim se pristupa mreži, ova aktivnost je isključivo u nadležnosti administratora preduzeća.
2. Korisnički nalog se isključivo koristi u poslovne svrhe, onako kako je definisano radnim mestom nosioca korisničkog naloga. Posebno se zabranjuje:
   - emitovanje sadržaja koji kompromituju autoritet Preduzeća i ličnosti na profesionalnoj, verskoj, nacionalnoj, rasnoj i političkoj osnovi
   - neadekvatno korišćenje mrežnih servisa i komunikacione opreme, kao što je zagušivanje saobraćaja, promene na softverskim instalacijama, promene radnih parametara i tome slično.
3. Nije dozvoljeno narušavanje privatnosti podataka kao i sprovođenje aktivnosti koje mogu da ugroze integritet podataka u bilo kom obliku.

3.2.3 Ukidanje korisničkih naloga

Član 30.

Administrator preduzeća je zadužen za evidenciju i praćenje upotrebe korisničkih naloga i njihovo ažuriranje.

U slučaju nekorektnog korišćenja mrežnih resursa, može se nosiocu naloga zabraniti pristup na određeno vreme. Administrator preduzeća radi arhiviranje.
Administrator preduzeća ima ekskluzivno pravo da bez prethodne saglasnosti direktora privremeno ukine korisnički nalog, ukoliko proceni da je to u interesu bezbednosti informaciono-komunikacinog sistema Preduzeća.

Administrator je zadužen za ukidanje korisničkog naloga u slučaju:

1. prekida radnog odnosa nosioca naloga (informaciju dostavlja pravna služba);
2. postoji odluka o zabrani korišćenja mreže Preduzeća.

4. PRAVILA O BEZBEDNOSTI I ZAŠTITI KORIŠĆENJA PODATAKA I INFRASTRUKTURE INFORMACIONO-KOMUNIKACIONOG SISTEMA JKP "VODOVDO I KANALIZACIJA" POŽAREVAC

JKP „Vodovod i kanalizacija" Požarevac, Dr. Voje Dulića 4, Požarevac, tel. 012/555-801, email. office@vodovod012.rs

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

Član 31.

Prostor u kome se nalaze serveri, mrežna ili komunikaciona oprema IKT sistema, organizuje sa kao administrativna zona. Administrativna zona se uspostavlja za fizički pristup resursima IKT sistema u kontrolisanom, vidljivo označenom prostoru, koji je obezbeđen mehaničkom bravom.

Prostor mora da bude obezbeđen od kompromitujućeg elektromagnetnog zračenja (KEMZ), požara i drugih elementarnih nepogoda, i u njemu treba da bude odgovarajuća temperatura (klimatizovan prostor).

4.2 Zaštita od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT system

Član 32.

Ulaz u prostoriju u kojoj se nalazi IKT oprema, dozvoljen je samo administratoru IKT sistema/zaposlenima na poslovima IKT.

Osim administratora sistema, pristup administrativnoj zoni mogu imati i treća lica u cilju instalacije i servisiranja određenih resursa IKT sistema, a po prethodnom odobrenju direktora i uz prisustvo nadležnog lica administratora preduzeća.

Pristup administrativnoj zoni može imati i zaposleni/a na poslovima održavanja higijene uz prisustvo nadležnog lica tj. administratora preduzeća.

Član 33.

Prostorija mora biti vidljivo obeležena u kojoj se nalazi IKT oprema i mediji sa podacima.

Prozori i vrata na ovoj prostoriji 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, 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 direktora.

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

Ako se oprema iznosi radi servisiranja, pored odobrenja direktora, 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 mora biti definisana obaveza zaštite podataka koji se nalaze na medijima koji su deo IKT resursa Preduzeća.

4.3 Obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka

Član 34.

Zaposleni 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 direktoru 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 zaposlenih-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.

4.4 Zaštita podataka i sredstva za obradu podataka od zlonamernog softvera

Član 35.

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 prenosnim medijima (USB memorija, CD itd.), instalacijom ne licenciranog softvera i sl.

Za uspešnu zaštitu od virusa na svakom računaru je instaliran antivirusni program. Svakodnevno se automatski vrši dopuna antivirusnih definicija.

Zabranjeno je zaustavljanje i isključivanje antivirusnog softvera tokom skeniranja prenosnih medija.

Prenosivi mediji, pre korišćenja, moraju biti provereni na prisustvo virusa. Ako se utvrdi da prenosivi medij sadrži viruse, ukoliko je to moguće, vrši se čišćenje medija antivirusnim softverom. Rizik od eventualnog gubitka podataka prilikom čišćenja medija od virusa snosi donosilac medija.

Član 36.

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 preduzeća 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 zaposleni-korisnik priključuje na Internet mora biti odgovarajuće podešen i zaštićen, pri čemu podešavanje vrši administrator preduzeća.

Član 37.

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 adminstratoru preduzeća.

Član 38.

Zaposlenima je zabranjeno gledanje filmova i igranje igrica na računarima i "krstarenje" WEB stranicama koje sadrže nedoličan sadržaj, kao i samovoljno preuzimanje istih sa interneta (torenti i drugi slični programi).

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.

4.5 Zaštita od gubitka podataka

Član 39.

Baze podataka obavezno se arhiviraju na prenosive medije (DVD, USB, eksterni hard disk), najmanje jednom 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 40.

Dnevno kopiranje-arhiviranje vrši se za svaki radni dan u sedmici, od 11:00 i 15:05 časova svakog radnog dana.

Nedeljno kopiranje-arhiviranje vrši se poslednjeg radnog dana u nedelji, od 11:00 i 15 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 15 časova.

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

Član 41.

Svaki primerak prenosnog informatičkog medija sa kopijama-arhivama, mora biti označen brojem, datumom izrade kopije-arhive. Kopije-arhive se čuvaju u prostoriji koja je fizički i u skladu sa merama zaštite od požara obezbeđena.

Kopije-arhive se izrađuju u dva primerka, od kojih se jedan čuva u prostoriji u kojoj se čuvaju kopije-arhive a drugi primerak eksternim back up hard diskovima.

Ispravnost kopija-arhiva proverava se i to tako što se izvrši povraćaj baza podataka koje se nalaze na mediju, pri čemu vraćeni podaci nakon povraćaja treba da budu ispravni i spremni za upotrebu.

Član 42.

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

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

Po prijemu prijave administrator preduzeća je dužan da odmah obavesti direktora i preduzme mere u cilju zaštite resursa IKT sistema.

Administrator preduzeća vodi evidenciju o prijavama incidenata, na osnovu kojih, protiv odgovornog lica, može se pokrenuti disciplinski, prekršajni ili krivični postupak.

Član 43.

Izmene i dopune ovog pravilnika vrše se po postupku i na način za njegovo donošenje.

Član 44.

Pravilnik stupa na snagu 8. dana od dana objavljivanja na oglasnoj tabli JKP „Vodovod i kanalizacija" Požarevac, od kada će se i primenjivati.

JKP „Vodovod i kanalizacija" Požarevac
Direktor

Aleksandar Dimitrijević, dipl.ing.tehnologije