Republika Srbija
PREKRŠAJNI SUD
SU I-52/17
08.06.2017. godine
U Ž I C E

Na osnovu člana 8. Zakona o informacionoj bezbednosti ("Službeni glasnik RS", broj 6/16), članova 1-8 Uredbe o bližem sadržaju akta o bezbednosti informaciono komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionih sistema od posebnog značaja ("Službeni glasnik RS", broj 94/16 od 24.11.2016. godine), predsednik Prekršajnog suda u Užicu, donosi:

P R A V I L N I K
O BEZBEDNOSTI INFORMACIONO – KOMUNIKACIONIH SISTEMA PREKRŠAJNOG SUDA U UŽICU

I.Uvodne odredbe

Član 1

Ovim pravilnikom bliže se definišu mere zaštite informaciono-komunikacionih sistema u Prekršajnom sudu u Užicu, a naročito principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i dužnosti i odgovornosti korisnika informaciono-komunikacionih sistema (u daljem tekstu IKT sistem).

Član 2

Ciljevi donošenja ovog Pravilnika su:
doprinos podizanju opšte svesti o rizicima i opasnostima koje su vezane za korišćenje informacionih tehnologija;
minimizacija bezbednosnih incidenata;
doprinos razvoju odgovarajućih bezbednosnih aplikacija i
obezbeđivanje konzistentne kontrole svih komponenata IKT sistema.

Član 3

Ovaj Pravilnik je obavezujući za sve unutrašnje organizacione jedinice Prekršajnog suda u Užicu i za sve korisnike informatičkih resursa, kao i za sva treća lica koja koriste informatičke resurse suda.

Nepoštovanje ovog Pravilnika povlači disiplinsku odgovornost korisnika informatičkih resursa.

Za praćenje primene ovog Pravilnika nadležan je predsednik suda i sudska uprava.

Član 4

Pojedini pojmovi u smislu ovog pravilnika imaju sledeće značenje:

1. informaciono-komunikacioni sistem (IKT sistem) je tehnološko-organizaciona celina koja obuhvata: elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije;

uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno da se u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa; podatke koji se pothranjuju, obrađuju, pretražuju ili prenose u svrhu njihovog rada, upotrebe, zaštite ili održavanja; organizacionu strukturu putem koje se upravlja IKT sistemom;

2. informaciona bezbednost predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica;

3. tajnost je svojstvo koje znači da podatak nije dostupan neovlašćenim licima;

4. integritet znači očuvanost izvornog sadržaja i kompletnosti podataka;

5. raspoloživost je svojstvo koje znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban;

6. autentičnost je svojstvo koje znači da je moguće proveriti i potvrditi da je podatak stvorio ili poslao onaj za koga je deklarisano da je tu radnju izvršio;

7. neporecivost predstavlja sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći;

8. rizik znači mogućnost narušavanja informacione bezbednosti, odnosno mogućnost narušavanja tajnosti, integriteta, raspoloživosti, autentičnosti ili neporecivosti podataka ili narušavanja ispravnog funkcionisanja IKT sistema;

9. upravljanje rizikom je sistematičan skup mera koji uključuje planiranje, organizovanje i usmeravanje aktivnosti kako bi se obezbedilo da rizici ostanu u propisanim i prihvatljivim okvirima;

10. incident je unutrašnja ili spoljna okolnost ili događaj kojim se ugrožava ili narušava informaciona bezbednost;

11. mere zaštite IKT sistema su tehničke i organizacione mere za upravljanje bezbednosnim rizicima IKT sistema;

12. tajni podatak je podatak koji je, u skladu sa propisima o tajnosti podataka, određen i označen odgovarajućim stepenom tajnosti;

13. Kriptobezbednost je komponenta informacione bezbednosti koja obuhvata kriptozaštitu, upravljanje kriptomaterijalima i razvoj metoda kriptozaštite;

14. informaciona dobra obuhvataju podatke u datotekama i bazama podataka, programski kod, konfiguraciju hardverskih komponenata, tehničku i korisničku dokumentaciju, unutrašnje opšte pravilnike, procedure i slično;

15. VPN (Virtual Private Network) je „privatna" komunikaciona mreža koja omogućava korisnicima na razdvojenim lokacijama da preko javne mreže jednostavno održavaju zaštićenu komunikaciju;

16. WAN (Wide Area Network) je mreža širokog područja koja pokriva veće zemljopisno područje(gradove, države ili kontinente) i obično se koristi za međusobno povezivanje udaljenih računara ili lokalnih (LAN) mreža.

17. Administrator IKT sistema - lice koje ima administratorski nalog koji omogućava pristup i administraciju informatičkih resursa samo sa jednim korisničkim nalogom, kao i unošenje i izmenu svih ostalih korisničkih naloga.

18. Vaskur je rezervna kopija podataka;

19. Download je transfer podataka sa centralnog računara ili web prezentacije na lokalni računar;

20. MAC adresa (Media Access Control Address) je jedinstven broj, kojim se vrši identifikacija uređaja na mreži;

21. UPS (Uninterruptible power supply) je uređaj za neprekidno napajanje električnom energijom;

22. Freeware je besplatan softver;

23. Opensource softver otvorenog koda;

24. Firewall je „zaštitni zid“ odnosno sistem preko koga se vrši nadzor i kontroliše protok informacija između lokalne mreže i interneta u cilju onemogućavanja zlonamernih aktivnosti;

25. USB ili fleš memorija je spoljni medijum za skladištenje podataka;

26. CD-ROM (Compact disk – read only memory) koristi se kao medijum za skladištenje podataka;

27. DVD je optički disk visokog kapaciteta koji se koristi za skladištenje podataka.

II. Mere zaštite

Član 5

Merama zaštite se obezbeđuje prevencija od nastanka incidenata koji ugrožavaju obavljanje delatnosti Prekršajnog suda u Užicu, odnosno zaštita podataka sadržanih u IKT sistemu od neovlašćenog pristupa, modifikacije, korišćenje i destrukcije, na način da integritet, tajnost i raspoloživost podataka ne smeju biti kompromitovani.

Organizaciona struktura, sa utvrđenim poslovima i odgovornostima zaposlenih, kojima se ostvaruje upravljanje informacionom bezbednošću u Prekršajnom sudu u Užicu.

Član 6

Svaki zaposleni-korisnik resursa IKT sistema je odgovoran za bezbednost resursa IKT sistema koje koristi radi obavljanja poslova iz svoje nadležnosti.

Za kontrolu i nadzor nad obavljanjem poslova zaposlenih-korisnika, u cilju zaštite i bezbednosti IKT sistema, kao i za obavljanje poslova iz oblasti bezbednosti celokupnog IKT sistema nadležan je sistem administrator Prekršajnog suda u Užicu.

Član 7

Zaposleni-korisnici resursa IKT sistema, mogu putem mobilnih uređaja, koji su podešeni od strane sistem administratora, da pristupaju samo određenim delovima IKT sistema.

Mobilni uređaji moraju biti podešeni tako da omoguće siguran i bezbedan pristup.

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

Sistem administrator svakodnevno kontroliše pristup resursima IKT sistema i proverava ima li pristupa sa nepoznatih uređaja (sa nepoznatih MAC adresa) i ako se ustanovi neovlašćen pristup ta MAC adresa se unosi u „block“ listu softvera koji se koristi za kontrolu pristupa.

U slučaju kvara mobilnog uređaja, sistem administrator je dužan da pre predaje uređaja ovlašćenom servisu, uradi kopiju podataka koji se nalaze na mobilnom uređaju, a potom ih obriše iz uređaja, i po povratku iz servisa ponovo vrati podatke u mobilni uređaj.

Član 8

IKT sistemom upravljaju zaposleni u skladu sa važećom sistematizacijom radnih mesta.

Sistem administrator je dužan da svakog korisnika IKT resursa upozna sa odgovornostima i pravilima korišćenja IKT resursa Prekršajnog suda u Užicu.

Svako korišćenje IKT resursa Prekršajnog suda u Užicu od strane zaposlenog korisnika, van dodeljenih ovlašćenja, podleže disciplinskoj odgovornosti zaposlenog, kojom se definiše odgovornost za neovlašćeno korišćenje imovine.

Član 9

U slučaju promene poslova, odnosno nadležnosti korisnika-zaposlenog, administrator sistema će izvršiti promenu privilegija koje je korisnik-zaposleni imao u skladu sa opisom radnih zadataka, a na osnovu zahteva pretpostavljenog rukovodioca.

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

Korisnik IKT resursa, nakon prestanka radnog angažovanja u sudu, ne sme da otkriva podatke koji su od značaja za informacionu bezbednost IKT sistema.

Član 10

Informaciona dobra su svi resursi koji sadrže poslovne informacije Prekršajnog suda u Užicu, 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. Evidenciju o informacionim dobrima vodi sistem administrator u papirnoj ili elektronskoj formi.

Predmet zaštite obuhvata:

1. hardverske i softverske komponente informatičkih resursa
2. podatke koji se obrađuju ili čuvaju na informatičkim resursima
3. korisničke naloge i druge podatke o korisnicima informatičkih resursa u prekršajnom sudu

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

Član 11.

Podaci koji se nalaze u IKT sistemu predstavljaju poslovnu tajnu i kao takvi moraju biti zaštićeni u skladu sa odredbama Uredbe o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima („Sl. Glasnik RS", br. 53/2011).

Član 12

Podaci mogu da se snime (arhiviraju, zapišu) na serveru na kome se snimaju podaci, u folderu nad kojim će pravo pristupa imati samo zaposleni-korisnici kojima je to pravo obezbeđeno odlukom predsednika suda.

Podaci i dokumenti mogu da se snime na druge nosače (eksterni hard disk, USB, CD, DVD) samo od strane ovlašćenih zaposlenih-korisnika.

Nosači informacija moraju biti propisano obeleženi i odloženi na mesto na kome će biti zaštićeni od neovlašćenog pristupa.

U slučaju transporta nosača informacija predsednik suda će odrediti odgovornu osobu i način transporta.

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

Član 13

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

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

Zaposleni-korisnik dužan je da poštuje i sledeća pravila bezbednog i primernog 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 Prekršajnog suda u Užicu;
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 podataka u skladu sa propisanim procedurama;
13. koristi internet i elektronsku poštu u skladu sa propisanim procedurama;
14. prihvati da svi pristupi informatičkim resursima i informacijama treba da budu zasnovani na principu minimalne neophodnosti;
15. 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;
16. ne sme da instalira, modifikuje, isključuje iz rada ili briše zaštitni, sistemski ili aplikativni softver.

Član 14

Pravo pristupa imaju samo zaposleni-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 može da koristi isključivo sistem administrator prekršajnog suda.

Korisnički nalog se sastoji od korisničkog imena i lozinke 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 u saradnji sa neposrednim rukovodiocem, a u skladu sa potrebama obavljanja poslovnih zadataka od strane zaposlenog-korisnika.

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

Član 15

Korisnički nalog se sastoji od korisničkog imena i lozinke.

Korisničko ime se kreira latiničnim pismom po matrici (prvo slovo imena i celo prezime) kao jedna reč razdvojeno jedino tačkom i bez upotrebe slova đ, ž, lj, nj, ć, č, dž, š.

Lozinka mora da sadrži minimum osam karaktera, sastavljenih kombinacijom latiničnih velikih i malih slova kao i brojeva. 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.

Zaposleni-korisnik dužan je da menja lozinku jednom mesečno i ista lozinka ne sme da se ponavlja 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).

Deo prijavljivanja u IKT sistem Prekršajnog suda u Užicu vrši se ubacivanjem medija sa elektronskim sertifikatom u čitač kartice. Neovlašćeno ustupanje korisničkog naloga kao i medija sa elektronskim sertifikatom drugom licu, podleže disciplinskoj odgovornosti.

Član 16

U cilju fizičke sigurnosti informatičkih resursa moraju se obezbediti sledeći uslovi:

1. serveri, storidži i komunikaciono čvorište u prostorijama suda moraju biti smešteni u posebnoj prostoriji (server sobi), koja ispunjava standarde protivpožarne zaštite i poseduje

neprekidno napajanje električnom energijom i adekvatnu klimatizaciju i kojoj je zabranjen pristup nezaposlenim licima;

2. pristup server sobi, pored lica koja su zadužena za održavanje IKT sistema, mogu imati i druga lica, uz prethodno odobrenje predsednika suda;

3. radna stanica mora da bude primerno fizički obezbeđena sa ciljem detekcije i onemogućavanja fizičkog pristupa ili oštećenja kritičnih komponata;

4. prostorije u kojima se trenutno ne boravi moraju biti obezbeđene od neovlašćenog fizičkog pristupa;

5. štampači, kopir mašine i faks mašine moraju biti locirane unutar fizički bezbedne zone, radi sprečavanja neovlašćenog kopiranja i prenosa osetljivih informacija;

6. mediji sa poverljivim podacima moraju biti zaštićeni od neautorizovanog pristupa i pregleda.

Član 17

Ulaz u prostorije u kojoj se nalazi IKT oprema, dozvoljen je samo administratoru IKT sistema i zaposlenim-korisnicima IKTsistema. Osim administratora sistema, pristup administrativnoj zoni mogu imati i treća lica u cilju instalacije i servisiranja određenih resursa IKT sistema, a po prethodnom odobrenju predsednika suda i uz prisustvo nadležnog lica.

Pristup administrativnoj zoni mogu imati i lica koja pružaju usluge održavanja higijene uz prisustvo nadležnog lica.

Administrativna zona mora imati protivpožarnu opremu koja se koristi samo u slučaju požara u prostoriji u kojoj se nalazi IKT oprema i mediji sa podacima. Serveri i aktivna mrežna oprema (switch, modem, router, firewall) moraju stalno biti priključeni na uređaje za neprekidno napajanje električnom energijom - UPS.

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

IKT oprema se u slučaju opasnosti (požar, vremenske nepogode i sl.) može izneti i bez odobrenja predsednika suda.

U slučaju iznošenja opreme radi selidbe ili servisiranja, neophodno je odobrenje predsednika suda koji će odrediti uslove, način i mesto iznošenja opreme. Ako se oprema iznosi radi servisiranja, pored odobrenja predsednika suda sistem administrator je dužan da sačini zapisnik u kome se navodi naziv i tip opreme, serijski broj, naziv servisera i kratak opis kvara.

Ugovorom sa serviserom mora biti definisana obaveza zaštite podataka koji se nalaze na medijima koji su deo IKT resursa Prekršajnog suda u Užicu.

Član 18

Zaposleni na poslovima IKT sistema 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 predsedniku suda odgovarajuće mere.

Pre uvođenja u rad novog softvera neophodno je napraviti kopiju arhive 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 sučaju 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.

Član 19

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 memorije, CD itd.), instalacijom nelicenciranog softvera i sl. Za uspešnu zaštitu od zlonamernog softvera Prekršajni sud u Užicu svoju delatnost obavlja preko „Pravosudne“ WAN mreže koja ima ograničen pristup, takođe na svakom računaru je instaliran antivirusni program koji se svakodnevno automatski ažurira.

U cilju zaštite od IKT sistema od malicioznog softvera neophodna je primena licenciranog softvera, odnosno zabrana neautorizovanog softvera. Prenosivi mediji pre korišćenja moraju biti provereni na prisustvo virusa. Ako se utvrdi da prenosivi medij sadrži viruse, vrši se čišćenje medija od virusa, uz saglasnost donosioca medija.

Rizik od eventualnog gubitka podataka prilikom čišćenja medija antivirusnim softverom, snosi donosilac medija.

Zaposlenim-korisnicima koji su priključeni na IKT sistem, strogo je zabranjeno samostalno priključivanje na internet (priključivanje preko sopstvenog modema) kao i nedozvoljena upotreba interneta koja obuhvata:

instaliranje, distribuciju, oglašavanje, prenos ili na drugi način činjenje dostupnim „piratskih“ ili drugih softverskih proizvoda koji nisu licencirani na ogovarajući 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;

preuzimanja (download) podataka velike „težine“ koji prouzrokuju „zagušenje“ na mreži;

preuzimanje (download) materijala zaštićenih autorskim pravima;

korišćenje linkova koji nisu u vezi sa poslom (gledanje filmova, audio i videostriming i sl.);

nedozvoljen pristup sadržaju, promena sadržaja, brisanje ili prerada sadržaja preko interneta.

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

U cilju sigurnosti korišćenja servisa elektronske pošte moraju se poštovati sledeća pravila:

elektronska pošta sa prilozima ne sme se otvarati ako dolazi sa sumljivih i nepoznatih adresa, već se mora izbrisati;

zabranjeno je korišćenje elektronske pošte u privatne svrhe (ne smeju se koristiti poslovni nalozi elektronske pošte u privatne svrhe).

Član 20

Zaštita od gubitka podataka u Prekršajnom sudu u Užicu obezbeđuje se kreiranjem rezervnih kopija na eksternom disku koji je propisano obeležen i čuva se na obezbeđenom mestu.

Svaka radna stanica ima konfigurisan sekundarni hard disk na kome se kopiraju podaci. Svi dokumenti štampani iz IKT sistema se memorišu kao PDF dokumenti.

Član 21

U IKT sistemu može da se instalira samo softver za koji postoji važeća licenca, odnosno Freewere i Opensource verzije.

Inastalaciju i podešavanje softvera može da vrši samo sistem administrator Prekršajnog suda u Užicu. 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.

Član 22

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

Podešavanjem korisničkih polisa od strane sistem administratora onemogućeno je instaliranje softvera koji može dovesti do ugrožavanja bezbednosti IKT sistema.

Član 23

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

Član 24

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) mora biti obezbeđena i locirana na propisanim mestima, dostupna sistem administratoru koje je dužan da vrši kontrolu celokupne mrežne opreme i blagovremeno preuzima mere u cilju otklanjanja eventualnih nepravilnosti.

Bezžična mreža koju mogu koristiti posetioci objekta u nadležnosti Prekršajnog suda u Užicu mora biti odvojena od interne mreže koju koriste zaposleni-korisnici suda, kroz koju se vrši razmena službenih podataka.

Član 25

Prenosivi mediji koji sadrže podatke moraju da budu propisano obeleženi i popisani.

Prenos medija kao i način prenosa unutar i van operatora IKT sistema određuje predsednik suda. Prenosivi mediji pre stavljanja van upotrebe moraju biti fizički uništeni.

Član 26

Način instaliranja novih, zamena i održavanje postojećih resursa IKT sistema spada u delokrug poslova sistem administratora, dok su isti poslovi sa trećim licima definisani ugovorom sklopljenim sa tim licima.

Predsednik suda je zadužen za tehnički nadzor nad realizacijom ugovorenih obaveza od strane trećih lica ili za tu vrstu posla može ovlasti drugo lice (sistem administratora).

O uspostavljanju novog IKT sistema, odnosno uvođenju novih delova i izmenama postojećih delova IKT sistema, administrator sistema mora da vodi dokumentaciju koja sadrži opise svih urađenih procedura.

Član 27

U slučaju bilo kakvog incidenta koji može da ugrozi bezbednost resursa IKT sistema, zaposleni-korisnik je dužan da odmah obavesti sistem administratora prekršajnog suda. Po prijemu prijave sistem administrator je dužan da o tome obavesti predsednika suda i preuzme mere u cilju zaštite resursa IKT sistema.

Sistem administrator 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.

Član 28

U slučaju vanrednih okolnosti, koje mogu da dovedu do izmeštanja IKT sistema iz zgrade suda sistem administrator 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 sistem administrator i to u tri primerka, od kojih je jedan kod njega, drugi kod nadležnog organa za poslove odbrane i vanredne situacije, a treći primerak kod predsednika suda.

Delovi IKT sistema koji nisu neophodni za funkcionisanje u vanrednim situacijama, skladište se na rezervnu lokaciju, koju odredi predsednik suda.

III. Izmena Pravilnika o bezbednosti

Član 29

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, sistem administrator je dužan da obavesti predsednika suda, 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 resursa IKT sistema.

IV. Provera IKT sistema

Član 30

Proveru IKT sistema vrši sistem administrator Prekršajnog suda u Užicu.

V. Sadržaj izveštaja o proveri IKT sistema

Član 31

Izveštaj o proveri 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;
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 adekvatne primene predviđenih mera zaštite u operativnom radu;
8. ocena ukupnog nivoa informacione bezbednosti;
9. predlog eventualnih korektivnih mera; 10. potpis odgovornog lica koje je sprovelo proveru IKT sistema.

VI. Prelazne i završne odredbe

Član 32

Pravilnik stupa na snagu narednog dana od dana objavljivanja na oglasnoj tabli Prekršajnog suda u Užicu.

Pravilnik je objavljen na oglasnoj tabli Prekršajnog suda u Užicu dana 08.06.2017. godine.

Užice, dana 08.06.2017. godine.

Predsednik suda
Slobodan Marinković