Na osnovu člana 8. Zakona o informacionoj bezbednosti ("Sl. glasnik RS", br. 6/2016 i 94/2017) i člana 2. Uredbe o bližem sadržaju Akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionog sistema od posebnog značaja ("Sl. glasnik RS", br. 94/2016), Upravni odbor Doma zdravlja Tutin je na 21. sednici održanoj 31.10.2019. godine doneo:

PRAVILNIK O UPRAVLJANJU INFORMACIJAMA (PODACIMA) I BEZBEDNOSTI INFORMACIONO-KOMUNIKACIONOG SISTEMA DOMA ZDRAVLJA TUTIN

Uvodne odredbe

Član 1.

Ovim pravilnikom, u skladu sa Zakonom o informacionoj bezbednosti i Uredbom o bližem sadržaju Akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti informaciono-komunikacionog sistema od posebnog značaja, utvrđuju se mere zaštite, principi, način i procedure u vezi sa bezbednošću i resursima informaciono-komunikacionih sistema Doma zdravlja Tutin (u daljem tekstu: Dom zdravlja).

Član 2.

Mere propisane ovim pravilnikom se odnose na sve organizacione jedinice Doma zdravlja, na sve zaposlene – korisnike informatičkih resursa, kao i na treća lica koja koriste informatičke resurse Doma zdravlja.

Nepoštovanje odredbi ovog pravilnika povlači disciplinsku odgovornost zaposlenog-korisnika informatičkih resursa Doma zdravlja.

Član 3.

Pojedini termini u smislu ovog pravilnika imaju sledeće značenje:

- 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 u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa;
  - podatke koji se pohranjuju, obrađuju, pretražuju ili prenose pomoću sredstava iz podtač. (1) i (2) ovog člana, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja;
  - organizacionu strukturu putem koje se upravlja IKT sistemom;

- 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;
- Tajnost je svojstvo koje znači da podatak nije dostupan neovlašćenim licima;
- Integritet znači očuvanost izvornog sadržaja i kompletnosti podatka;
- Raspoloživost je svojstvo koje znači da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban;
- 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;
- Neporecivost predstavlja sposobnost dokazivanja da se dogodila određena radnja ili da je nastupio određeni događaj, tako da ga naknadno nije moguće poreći;
- Rizik znači mogućnost narušavanja informacione bezbednosti, odnosno mogućnost narušavanja tajnosti, integriteta, raspoloživosti, autentičnosti ili neporecivosti podataka ili narušavanja ispravnog funkcionisanja IKT sistema;
- 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;
- Incident je unutrašnja ili spoljna okolnost ili događaj kojim se ugrožava ili narušava informaciona bezbednost;
- Mere zaštite IKT sistema su tehničke i organizacione mere za upravljanje bezbednosnim rizicima IKT sistema;
- Tajni podatak je podatak koji je, u skladu sa propisima o tajnosti podataka, određen i označen određenim stepenom tajnosti;
- IKT sistem za rad sa tajnim podacima je IKT sistem koji je u skladu sa zakonom određen za rad sa tajnim podacima;
- Kompromitujuće elektromagnetno zračenje (KEMZ) predstavlja nenamerne elektromagnetne emisije prilikom prenosa, obrade ili čuvanja podataka, čijim prijemom i analizom se može otkriti sadržaj tih podataka;
- Kriptobezbednost je komponenta informacione bezbednosti koja obuhvata kriptozaštitu, upravljanje kriptomaterijalima i razvoj metoda kriptozaštite;
- Kriptozaštita je primena metoda, mera i postupaka radi transformisanja podataka u oblik koji ih za određeno vreme ili trajno čini nedostupnim neovlašćenim licima;
- Kriptografski proizvod je softver ili uređaj putem koga se vrši kriptozaštita;
- Kriptomaterijali su kriptografski proizvodi, podaci, tehnička dokumentacija kriptografskih proizvoda, kao i odgovarajući kriptografski ključevi;
- Bezbednosna zona je prostor ili prostorija u kojoj se, u skladu sa propisima o tajnosti podataka, obrađuju i čuvaju tajni podaci;
- Informaciona dobra obuhvataju podatke u datotekama i bazama podataka, programski kod, konfiguraciju hardverskih komponenata, tehničku i korisničku dokumentaciju, unutrašnje opšte pravilnike, procedure i slično;
- VPN (Virtuelna privatna mreža) je „privatna" komunikaciona mreža koja omogućava korisnicima na razdvojenim lokacijama da preko javne mreže jednostavno održavaju zaštićenu komunikaciju;
- MAC adresa (Media Access Control Adress) je jedinstven broj, kojim se vrši identifikacija uređaja na mreži;
- BackUp je rezervna kopija podataka;

- Download je transfer podataka sa centralnog računara ili web prezentacije na lokalni računar;
- UPS (Uninterruptible power supply) je uređaj za neprekidno napajanje električnom energijom;
- Freeware je besplatan softver;
- Opensource softver otvorenog koda;
- 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;
- USB ili fleš memorija je spoljašnji medijum za skladištenje podataka;
- CD-ROM (Compact disc – Read only memory) se koristi kao medijum za snimanje podataka;
- DVD je optički disk visokog kapaciteta koji se koristi kao medijum za skladištenje podataka;
- Informacija je korisni podatak koji može da utiče na nečije odluke i ponašanje, ima kontekst.

Mere zaštite

Član 4.

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

Član 5.

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 Doma zdravlja nadležni su angažovani informatičari Doma zdravlja, u skladu sa sistematizacijom radnih mesta u Domu zdravlja.

Kršenje bezbednosnih procedura u IKT sistemu zaposleni-korisnik je dužan da prijavi angažovanim informatičarima Doma zdravlja, a oni su dužni da preduzmu odgovarajuće mere.

Član 6.

Pod poslovima iz oblasti bezbednosti utvrđuju se:

- poslovi zaštite informacionih dobara, odnosno sredstava imovine za nadzor nad poslovnim procesima od značaja za informacionu bezbednost,
- poslovi onemogućavanja, odnosno sprečavanja neovlašćene ili nenamerne izmene, oštećenja ili zloupotrebe sredstava, odnosno informacionih dobara IKT sistema Doma zdravlja, kao i pristup, izmene ili korišćenje sredstava bez ovlašćenja i bez evidencije o tome.

U slučaju incidenta angažovani informatičari Doma zdravlja, obaveštavaju direktora Doma zdravlja (u daljem tekstu: direktor), koji u skladu sa propisima obaveštava nadležne organe u cilju rešavanja.

Upravljanje informacijama

Član 7.

Svojinska i autorska prava nad informacijma (podacima) i softverom koji su kreirani korišćenjem IKT resursa Doma zdravlja pripadaju Domu zdravlja.

Direktor zaključno sa rukovodiocem službe u kojoj je informacija (podatak) kreirana, prikupljena ili se obrađuje je vlasnik podatka.

Svi podaci nezavisno od forme u kojoj se nalaze, a Dom zdravlja ih razmenjuje, čuva ili obrađuje na IKT resursima, klasifikuju se prema stepenu poverljivosti podatka.

Zaposleni koji koristi klasifikovane podatke odgovoran je za postupanje sa njima i dužan je da ih štiti u svim fazama korišćenja.

Član 8.

Nakon što je podatak klasifikovan kao strogo poverljiv ili poverljiv kreiran, sve nepotrebne verzije podatka, nastale tokom kreiranja, brišu se sa radne stanice ili se uništava (secka, cepa) papir na kome je štampana.

Obrada podataka vrši se u saglasnosti sa vlasnikom podatka i rukovodiocima nadležnim za oblast obrade informacija.

Podaci u elektronskoj formi klasifikovani kao strogo poverljivi ili poverljivi čuvaju se na serverima za čuvanje i razmenu podataka u direktorijumima sa ograničenim pravima pristupa.

Član 9.

Slanje podataka klasifikovanih kao strogo poverljivi ili poverljivi odobrava vlasnik podataka.

Strogo poverljivi podaci u elektronskoj formi šalju se šifrovani.

Strogo poverljivi ili poverljivi podaci pre smeštanja na prenosivi medijum se šifruju.

U slučaju ličnog dostavljanja ovlašćenom licu strogo poverljivih ili poverljivih podataka na prenosivom medijumu, ne vrši se šifrovanje.

Član 10.

Uništavanje strogo poverljivih ili poverljivih podataka smeštenih na hard disku vrši se korišćenjem softvera za bezbedno brisanje diska od strane ovlašćenih lica za informacione tehnologije.

Uništavanje strogo poverljivih ili poverljivih podataka smeštenih na prenosivom uređaju ili medijumu vrši se formatiranjem uređaja ili uništenjem uređaja ili medijuma.

Bezbednost rada na daljinu i upotreba mobilnih uređaja

Član 11.

Neregistrovani korisnici, putem mobilnih uređaja mogu da pristupe samo onim delovima mreže koji su konfigurisani tako da omogućavaju pristup Internetu ali ne i delovima mreže kroz koju se obavlja službena komunikacija.

Zaposleni-korisnici resursa IKT sistema, mogu putem mobilnih uređaja, koji su u vlasništvu Doma zdravlja i koji su podešeni od strane angažovanih informatičara Doma zdravlja, da pristupaju samo onim delovima IKT sistema koji im omogućavaju obavljanje radnih zadataka u okviru njihove nadležnosti (elektronska pošta, zdravstveni informacioni sistem i poslovni informacioni sistem), a na osnovu pisane saglasnosti direktora.

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.

Pristup resursima IKT sistema Doma zdravlja sa udaljenih lokacija, od strane zaposlenih-korisnika, u cilju obavljanja radnih zadataka, omogućen je putem zaštićene VPN/internet konekcije.

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

Angažovani informatičari Doma zdravlja, svakodnevno kontrolišu pristup resursima IKT sistema i proveravaju da li ima pristupa sa nepoznatih uređaja (sa nepoznatih MAC adresa).

Razmena elektronske pošte

Član 12.

Razmena elektronske pošte u Domu zdravlja dozvoljena je isključivo preko sistema za razmenu elektronske pošte i dokumenata.

Sistem za razmenu elektronske pošte ne sme da se koristi za kreiranje ili distribuciju neželjenih poruka.

Elektronske poruke ili drugi elektronski podaci, koji pokušavaju da sakriju identitet pošiljaoca ili da predstave pošiljaoca kao nekog drugog, nisu dozvoljeni.

Član 13.

Zabranjena je upotreba službene adrese elektronske pošte za razmenu poruka:

- čiji je sadržaj uvredljiv, klevetnički ili zastrašujući prema bilo kome, kao i poruke koje su pogrdne za bilo kog pojedinca ili grupu,
- koje svojim sadržajem diskriminišu po bilo kom osnovu,
- kojima se otkriva poslovna tajna Doma zdravlja ili poslovnog partnera, te lični podaci korisnika usluga Doma zdravlja koji mogu da nanesu štetu Domu zdravlja bilo koje vrste,
- koje služe za političku ili drugu propagandu,
- koje svojim sadržajem ometaju zaposlene u radu i onemogućavaju redovnu razmenu poslovnih informacija (tzv. „lančane poruke“ i sl.).

Član 14.

Neželjena pošta se smešta u karantin. Korisnik se obaveštava o porukama koje su smeštene u karantin i omogućava mu se pristup karantinu.

Nije dozvoljeno slanje elektronskih poruka bez naslova ili poruka većih od propisane veličine. O svakoj promeni u korišćenju sistema za razmenu elektronske pošte korisnik se obaveštava elektronskim putem.

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

Član 15.

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

Svaki novozaposleni-korisnik IKT resursa treba da se upozna sa odgovornostima i pravilima korišćenja IKT resursa, odnosno omogućiti da svaki novozaposleni prilikom potpisivanja ugovora o radu potpiše da je upoznat i sa ovim pravilnikom.

Svako korišćenje IKT resursa Doma zdravlja od strane zaposlenog-korisnika, van dodeljenih ovlašćenja, podleže disciplinskoj odgovornosti zaposlenog kojom se definiše odgovornost za neovlašćeno korišćenje imovine.

Zaštita od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica korisnika IKT sistema

Član 16.

U slučaju promene poslova, odnosno nadležnosti korisnika-zaposlenog, angažovani informatičari Doma zdravlja 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.

O prestanku radnog odnosa ili radnog angažovanja, kao i promeni radnog mesta, diplomirani pravnik za pravne, kadrovske i administrativne poslove, je dužan da obavesti angažovane informatičare Doma zdravlja, radi ukidanja, odnosno izmene pristupnih privilegija tog zaposlenog-korisnika.

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

Identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu

Član 17.

Informaciona dobra Doma zdravlja su svi resursi koji sadrže poslovne informacije Doma zdravlja, odnosno, putem kojih se vrši izrada, obrada, čuvanje, prenos, brisanje i uništavanje podataka u IT 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.

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.

Zaštita nosača podataka

Član 18.

Angažovani informatičari Doma zdravlja, 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:

- 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 zaposleni-korisnici kojima je to pravo obezbeđeno odlukom načelnika i
- podaci i dokumenti (posebno oni sa oznakom tajnosti) mogu da se snime na druge nosače (eksterni hard disk, USB, CD, DVD) samo od strane ovlašćenih zaposlenih - korisnika. Evidenciju nosača na kojima su snimljeni podaci, vode angažovani informatičari Doma zdravlja i ti mediji moraju biti propisno obeleženi i odloženi na mesto na kome će biti zaštićeni od neovlašćenog pristupa.

U slučaju transporta medija sa podacima, direktor će odrediti odgovornu osobu i način transporta.

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

Ograničenje pristupa podacima i sredstvima za obradu podataka

Član 19.

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 primerenog korišćenja resursa IKT sistema, i to da:

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

- obezbedi sigurnost podataka u skladu sa važećim propisima;
- pristupa informatičkim resursima samo na osnovu eksplicitno dodeljenih korisničkih prava;
- ne sme da zaustavlja rad ili briše antivirusni program, menja njegove podešene opcije, niti da neovlašćeno instalira drugi antivirusni program;
- na radnoj stanici ne sme da skladišti sadržaj koji ne služi u poslovne svrhe;
- izrađuje zaštitne kopije (backup) podataka u skladu sa propisanim procedurama;
- koristi internet i elektronsku poštu Doma zdravlja u skladu sa propisanim procedurama;
- prihvati da se određene vrste informatičkih intervencija (izrada zaštitnih kopija, ažuriranje programa, pokretanje antivirusnog programa i sl.) obavljaju u utvrđeno vreme;
- prihvati da svi pristupi informatičkim resursima i informacijama treba da budu zasnovani na principu minimalne neophodnosti;
- 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;
- ne sme da instalira, modifikuje, isključuje iz rada ili briše zaštitni, sistemski ili aplikativni softver.

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

Član 20.

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 mogu da koriste angažovani informatičari i menadžment.

Korisnički nalog se sastoji od korisničkog imena i lozinke, koji se mogu ukucavati ili čitati sa medija na kome postoji elektronski sertifikat, na osnovu koga/jih 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 i to tek nakon unosa podataka o zaposlenom u softver za upravljanje ljudskim resursima, 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 nadležnog rukovodioca.

Utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju

Član 21.

Korisnički nalog se sastoji od korisničkog imena i lozinke.

Lozinka mora da sadrži:

- broj karaktera lozinke mora biti veći od 8
- najmanje jedno veliko slovo
- najmanje jedan specijalan znak („#$%&/)
- najmanje jedan broj.

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 najmanje jednom u tri meseca, a najduže jednom u šest meseci.

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

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

Neovlašćeno ustupanje korisničkog naloga drugom licu, podleže disciplinskoj odgovornosti.

Predviđanje odgovarajuće upotrebe kriptozaštite radi zaštite tajnosti, autentičnosti odnosno integriteta podataka

Član 22.

Zaposleni-korisnici koriste kvalifikovane elektronske sertifikate za elektronsko potpisivanje dokumenata kao i autentifikaciju i autorizaciju pristupa pojedinim aplikacijama.

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

Zaposleni-korisnici su dužni da čuvaju svoje kvalifikovane elektronske sertifikate, kako ne bi došli u posed drugih lica.

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

Član 23.

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).

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

Član 24.

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 angažovanog informatičara Doma zdravlja.

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 mediji sa podacima.

Prozori i vrata na ovoj prostoriji moraju uvek biti zatvoreni.

Serveri i aktivna mrežna oprema (svič, 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 Doma zdravlja.

Obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka

Član 25.

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.

Zaštita podataka i sredstva za obradu podataka od zlonamernog softvera

Član 26.

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 nelicenciranog 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.

Direktor u dogovoru sa rukovodiocima organizacionih jedinica određuje 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 angažovani informatičari Doma zdravlja mogu da ukinu 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 angažovani informatičar Doma zdravlja.

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

Korisnik IKT resursa dužan je da, odmah prijavi neposrednom rukovodiocu svako uočavanje ili sumnju o nepravilnosti, ili nastanku nekog incidenta koji ugrožava rad IKT sistema. Slučaj se potom prijavljuje direktoru.

Strogo je zabranjeno gledanje filmova i igranje igrica 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.

Zaštita od gubitka podataka

Član 27.

Baze podataka obavezno se arhiviraju i na prenosive medije (CDROM, DVD, USB, eksterni hard disk), najmanje dva puta mesečno, za potrebe obnove baze podataka.

Baze podataka se repliciraju na više različitih lokacija, a jedna van prostorija Doma zdravlja.

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

Svaki primerak godišnje kopije-arhive čuva se u roku koji je definisan Uputstvom o kancelarijskom poslovanju organa državne uprave („Sl. glasnik RS", br. 10/1993, 14/1993-ispravka, 67/2016 i 3/2017).

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

Obezbeđivanje integriteta softvera i operativnih sistema

Član 28.

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

Instalaciju i podešavanje softvera mogu da vrše samo angažovani informatičari Doma zdravlja, odnosno zaposleni-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.

Zaštita od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema

Član 29.

Ukoliko se identifikuju slabosti koje mogu da ugroze bezbednost IKT sistema, informatičari Doma zdravlja su dužni da odmah izvrše podešavanje, odnosno instaliraju softver koji će otkloniti uočene slabosti.

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

Član 30.

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 direktora ustanove.

Zaštita podataka u komunikacionim mrežama uključujući uređaje i vodove

Član 31.

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.

Angažovani nformatičari Doma zdravlja su dužni da stalno vrše kontrolni pregled mrežne opreme i blagovremeno preduzimaju mere u cilju otklanjanja eventualnih nepravilnosti.

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

Član 32.

Kada se prenos podataka vrši između Doma zdravlja i drugog lica, mogu se zaključiti sporazumi o prenosu podataka i sporazumi o poverljivosti ili neotkrivanju koji sadrže odredbe o bezbednosti prenosa podataka.

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

Član 33.

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

Angažovani informatičari Doma zdravlja su zaduženi 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 angažovani informatičari Doma zdravlja vode dokumentaciju.

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

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

Član 34.

Prilikom testiranja sistema, podaci koji su označeni oznakom tajnosti, odnosno službenosti kao poverljivi podaci, ili su lični podaci, angažovani informatičari odgovaraju za podatke u skladu sa propisima kojima je definisana upotreba i zaštita takve vrste podataka.

Zaštita sredstava IKT sistema koja su dostupna pružaocima usluga

Član 35.

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.

Angažovani informatičari Doma zdravlja su odgovorni za kontrolu pristupa i nadzor nad izvršenjem ugovorenih obaveza, kao i za poštovanje odredbi ovog pravilnika kojima su takve aktivnosti definisane.

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

Član 36.

Dom zdravlja nema sklopljen ugovor sa trećim licima za pružanje usluga informacione bezbednosti.

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

Član 37.

U slučaju bilo kakvog incidenta koji može da ugrozi bezbednost resursa IKT sistema, zaposleni-korisnik je dužan da odmah obavesti angažovane informatičare Doma zdravlja.

Po prijemu prijave angažovani informatičari Doma zdravlja su dužni da odmah obaveste direktora Doma zdravlja i preduzmu 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), angažovani informatičari Doma zdravlja, su dužni da pored direktora obaveste i nadležni organ definisan ovom uredbom.

Angažovani informatičari Doma zdravlja vode 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.

Mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima

Član 38.

U slučaju vanrednih okolnosti, koje mogu da dovedu do izmeštanja IKT sistema, angažovani informatičari Doma zdravlja, su dužani da u najkraćem roku prenesu delove IKT sistema (ili obezbede funkcionisanje redudantnih komponenti na rezervnoj lokaciji ukoliko postoje) neophodne za funkcionisanje u vanrednoj situaciji na rezervnu lokaciju, u skladu sa planom reagovanja u vanrednim i kriznim situacijama.

Delove IKT sistema koji nisu neophodni za funkcionisanje u vanrednim situacijama, skladište se na rezervnu lokaciju, koju odredi direktor. 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 39.

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, angažovani informatičari Doma zdravlja su dužni da obaveste direktora, 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 IKT sistema.

Provera IKT sistema

Član 40.

Proveru IKT sistema vrše angažovani informatičari Doma zdravlja.

O izvršenoj proveri sačinjava se izveštaj, koji se dostavlja direktoru na uvid.

Prelazne i završne odredbe

Član 41.

Ovaj pravilnik objavljuje se na oglasnoj tabli i na veb prezentaciji Domu zdravlja.

Ovaj pravilnik stupa na snagu osam dana od dana objavljivanja na oglasnoj tabli Doma zdravlja.

ISTAKNUTO NA OGLASNOJ TABLI DOMA ZDRAVLJA TUTIN DANA 31.10.2019 GOD.

PREDSEDNIK UPRAVNOG ODBORA,
Emina Gusinac, dipl.ing.org.nauka, master