Na osnovu čl. 8. Zakona o informacionoj bezbednosti („Službeni glasnik RS", br. 6/2016, 94/2017 i 77/2019), čl. 2. Uredbe o bližem sadržaju Pravilnika o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, načinu provere informaciono-komunikacionih sistema od posebnog značaja i sadržaju izveštaja o proveri informaciono-komunikacionog sistema od posebnog značaja („Sl. Glasnik RS", br. 94/2016), čl. 26. st. 1. t. 13) Zakona o javnim preduzećima („Sl. glasnik RS", br. 15/2016 i 88/2019) i čl. 29. st. 1. t. 13) Statuta JKSP Senta (br.: 01-1927-09/2016 od 04.10.2016. god.), v. d. direktora Javnog komunalnog-stambenog preduzeća Senta, Akoš Slavnić, donosi

PRAVILNIK

o bezbednosti informaciono - komunikacionog sistema Javnog komunalno-stambenog preduzeća Senta

I. Uvodne odredbe

Član 1.

Ovim pravilnikom, u skladu sa Zakonom o informacionoj bezbednosti („Sl. glasnik RS", br. 6/2016, 94/2017 i 77/2019) i Uredbom o bližem sadržaju Pravilnika o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, način provere informaciono-komunikacionih sistema od posebnog značaja i sadržaj izveštaja o proveri informaciono-komunikacionog sistema od posebnog značaja („Sl. Glasnik RS", br. 94/2016), utvrđuju se mere zaštite, principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema Javnog komunalno-stambenog preduzeća Senta (u daljem tekstu: IKT sistem).

Član 2.

Mere propisane ovim pravilnikom se odnose na sve organizacione jedinice Javnog komunalno-stambenog preduzeća Senta, na sve zaposlene - korisnike informatičkih resursa, kao i na treća lica koja koriste informatičke resurse Javnog komunalno-stambenog preduzeća Senta.

Nepoštovanje odredbi ovog pravilnika povlači disciplinsku odgovornost zaposlenog-korisnika informatičkih resursa Javnog komunalno-stambenog preduzeća Senta.

Za praćenje primene ovog pravilnika obavezuje se "privredno-računovodstveni sektor" u Javnom komunalno-stambenom preduzeću Senta (dalje: P-R sektor).

Član 3.

Pojedini termini u smislu ovog pravilnika imaju sledeće značenje:

1) *informaciono-komunikacioni sistem* (IKT sistem) je tehnološko-organizaciona celina koja obuhvata:
   (1) elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije;
   (2) uređaje ili grupe međusobno povezanih uređaja, takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa;

(3) podatke koji se pohranjuju, obrađuju, pretražuju ili prenose pomoću sredstava iz podtač. (1) i (2) ove tačke, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja;

(4) 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 podatka;

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 određenim stepenom tajnosti;

13) *IKT sistem za rad sa tajnim podacima* je IKT sistem koji je u skladu sa zakonom određen za rad sa tajnim podacima;

14) *kompromitujuće elektromagnetno zračenje (KEMZ)* predstavlja nenamerne elektromagnetne emisije prilikom prenosa, obrade ili čuvanja podataka, čijim prijemom i analizom se može otkriti sadržaj tih podataka;

15) *kriptobezbednost* je komponenta informacione bezbednosti koja obuhvata kriptozaštitu, upravljanje kriptomaterijalima i razvoj metoda kriptozaštite;

16) *kriptozaštita* je primena metoda, mera i postupaka radi transformisanja podataka u oblik koji ih za određeno vreme ili trajno čini nedostupnim neovlašćenim licima;

17) *kriptografski proizvod* je softver ili uređaj putem koga se vrši kriptozaštita;

18) *kriptomaterijali* su kriptografski proizvodi, podaci, tehnička dokumentacija kriptografskih proizvoda, kao i odgovarajući kriptografski
ključevi;

19) *bezbednosna zona* je prostor ili prostorija u kojoj se, u skladu sa propisima o tajnosti podataka, obrađuju i čuvaju tajni podaci;

20) *informaciona dobra* obuhvataju podatke u datotekama i bazama podataka, programski kôd, konfiguraciju hardverskih komponenata, tehničku i korisničku dokumentaciju, unutrašnje opšte pravilnike, procedure i slično;

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

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

23) *Backup* je rezervna kopija podataka;

24) *Download* je transfer podataka sa centralnog računara ili web prezentacije na lokalni računar;
25) *UPS* (Uninterruptible power supply*)* je uređaj za neprekidno napajanje električnom energijom;
26) *Freeware* je besplatan softver;
27) *Opensource* je softver otvorenog koda;
28) *Firewall* je „zaštitni zid" odnosnosistem preko koga se vrši nadzor i kontroliše protok informacija između lokalne mreže i interneta u cilju onemogućavanja zlonamernih aktivnosti;
29) *USB ili fleš memorija* je spoljšnji medijum za skladištenje podataka;
30) *CD-ROM* (Compact disk - read only memory) se koristi kao medijum za snimanje podataka;
31) *DVD* je optički disk visokog kapaciteta koji se koristi kao medijum za skladištenje podataka;

II. Mere zaštite

Član 4.

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

1.Organizaciona struktura, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru Javnog komunalno-stambenog preduzeća Senta

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 Javnog komunalno-stambenog preduzeća Senta nadležan je P-R sektor, u skladu sa Pravilnikom o sistematizaciji radnih mesta u Javnom komunalno-stambenom preduzeću Senta (br. 01-983-09/2021-1 od 30.06.2021. godine – prečišćen tekst).

Član 6.

Pod poslovima iz oblasti bezbednosti utvrđuju se:

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

U slučaju incidenta, P-R sektor obaveštava direktora Javnog komunalno-stambenog preduzeća Senta, koji u skladu sa propisima obaveštava nadležne organe u cilju rešavanja nastalog bezbedonosnog incidenta.

2. Bezbednost rada na daljinu i upotreba mobilnih uređaja

Član 7.

Rad na daljinu i upotreba mobilnih uređaja u IKT sistemu nije omogućen.

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

Član 8.

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

P-R sektor je dužan da svakog novozaposlenog-korisnika IKT resursa upozna sa odgovornostima i pravilima korišćenja IKT resursa Javnog komunalno-stambenog preduzeća Senta, da ga upozna sa pravilima korišćenja resursa IKT sistema, kao i da vodi evidenciju o izjavama novozaposlenih – korisnika da su upoznati sa pravilima korišćenja IKT resursa.

Svako korišćenje IKT resursa Javnog komunalno-stambenog preduzeća Senta od strane zaposlenog-korisnika, van dodeljenih ovlašćenje, podleže disciplinskoj odgovornosti zaposlenog kojom se definiše odgovornost za neovlašćeno korišćenje imovine.

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

Član 9.

U slučaju promene poslova, odnosno nadležnosti korisnika-zaposlenog, P-R sektor 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, P-R sektor u saradnji sa neposrednim rukovodiocem je dužan da obavesti direktora Javnog komunalno-stambenog preduzeća Senta, radi ukidanja, odnosno izmene pristupnih privilegija tog zaposlenog-korisnika.

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

5. Identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu

Član 10.

Informaciona dobra Javnog komunalno-stambenog preduzeća Senta su svi resursi koji sadrže poslovne informacije Javnog komunalno-stambenog preduzeća Senta, 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 P-R sektor, u papirnoj ili elektronskoj formi.

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.

6. Klasifikovanje podataka tako da nivo njihove 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 tajnu, ako su tako definisani odredbama posebnim propisima.

Podaci koji se označe kao tajni, moraju biti zaštićeni u skladu sa odredbama Uredbe o posebnim merama zaštite tajnih podataka u informaciono-telekomunikacionim sistemima („Sl. Glasnik RS“, br. 53/2011).

7. Zaštita nosača podataka

Član 12.

P-R sektor 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 direktora;
- 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 na osnovu odluke direktora.

Evidenciju nosača na kojima su snimljeni podaci, vodi P-R sektor 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.

8. Ograničenje pristupa podacima i sredstvima za obradu podataka

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 primerenog korišćenja resursa IKT sistema, i to da:

1) koristi informatičke resurse isključivo u poslovne svrhe;
2) prihvati da su svi podaci koji se skladište, prenose ili procesiraju u okviru informatičkih resursa vlasništvo Javnog komunalno-stambenog preduzeća Senta i da mogu biti predmet nadgledanja i pregledanja;
3) postupa sa poverljivim podacima u skladu sa propisima, a posebno prilikom kopiranja i prenosa podataka;
4) bezbedno čuva svoje lozinke, odnosno da ih ne odaje drugim licima;
5) menja lozinke saglasno utvrđenim pravilima;
6) pre svakog udaljavanja od radne stanice, odjavi se sa sistema, odnosno zaključa radnu stanicu;
7) zahtev za instalaciju softvera ili hardvera podnosi u pisanoj formi, odobren od strane neposrednog rukovodioca;
8) obezbedi sigurnost podataka u skladu sa važećim propisima;
19) pristupa informatičkim resursima samo na osnovu eksplicitno dodeljenih korisničkih prava;
10) ne sme da zaustavlja rad ili briše antivirusni program, menja njegove podešene opcije, niti da neovlašćeno instalira drugi antivirusni program;
11) na radnoj stanici ne sme da skladišti sadržaj koji ne služi u poslovne svrhe;
12) izrađuje zaštitne kopije (backup) podataka u skladu sa propisanim procedurama;
13) koristi internet i elektronsku poštu u Javnom komunalno-stambenom preduzeću Senta u skladu sa propisanim procedurama;
14) prihvati da se određene vrste informatičkih intervencija (izrada zaštitnih kopija, ažuriranje programa, pokretanje antivirusnog programa i sl.) obavljaju u utvrđeno vreme;

15) prihvati da svi pristupi informatičkim resursima i informacijama treba da budu zasnovani na principu minimalne neophodnosti;
16) prihvati da tehnike sigurnosti (anti virus programi, firewall, sistemi za detekciju upada, sredstva za šifriranje, sredstva za proveru integriteta i dr.) sprečavaju potencijalne pretnje IKT sistemu.
17) ne sme da instalira, modifikuje, isključuje iz rada ili briše zaštitni, sistemski ili aplikativni softver.

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

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 samo zaposleni na poslovima "koordinator knjigovodstva AOP".

Administratorski nalog za upravljanje domenom može da koristi samo preduzeće/preduzetnik sa kojim JKSP Senta ima zaključen ugovor.

Adinistratorski nalog za upravljanje bazom podataka može da koristi samo preduzeće/preduzetnik sa kojim JKSP Senta ima zaključen ugovor.

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 zaposlenog na poslovima upravljanja ljudskim resursima, odnosno nadležnog rukovodioca.

10. Utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju

Član 15.

Korisnički nalog se sastoji od korisničkog imena i lozinke.

(Primer:Korisničko ime se kreira po matrici ime.prezime, latiničnim pismom bez upotrebe slova đ,ž,lj, nj, ć, č, dž, š.
(Preporuka: Umesto ovih slova koristiti slova iz tabele.)

Ćirilična slova	Latinična slova
Đ	dj
Ž	z
LJ	lj
NJ	nj
ć, č	c
Š	s
DŽ	dz

Lozinka mora da sadrži minimum (preporučeno) osam (ili upisati koliko) karaktera kombinovanih od malih i velikih slova, cifara i specijalnih znakova.

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

Ako 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 6 meseci.

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

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

Član 16.

Pristup resursima IKT sistema Javnog komunalno-stambenog preduzeća Senta ne zahteva posebnu kriptozaštitu.

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

Član 17.

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).

Evidenciju o ulasku u ovu zonu vodi P-R sektor.

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

Član 18.

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 rukovodioca P-R sektora.

Pristup administrativnoj zoni može imati i zaposleni/a na poslovima održavanja higijene uz prisustvo nadležnog lica rukovodioca P-R sektora.

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 (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 Javnog komunalno-stambenog preduzeća Senta.

14. Obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka

Član 19.

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.

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

Član 20.

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.

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

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.

U cilju zaštite, odnosno upada u IKT sistem Javnog komunalno-stambenog preduzeća Senta sa interneta, P-R sektor je dužan da održava sistem za sprečavanje upada.

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 P-R sektor 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 P-R sektor.

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 P-R sektoru.

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

16. Zaštita od gubitka podataka

Član 21.

Baze podataka obavezno se arhiviraju na prenosive medije (CDROM, DVD, USB, „strimer" traka, eksterni hard disk), najmanje jednom dnevno, nedeljno, mesečno i godišnje, za potrebe obnove baze podataka.

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

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

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

Nedeljno kopiranje-arhiviranje vrši se poslednjeg radnog dana u nedelji, od 20 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 20 časova.

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

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

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

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

Godišnje kopije-arhive se izrađuju u dva primerka, od kojih se jedan čuva u prostoriji u kojoj se čuvaju dnevne, nedeljne i mesečne kopije-arhive, a drugi primerak u sefu poslovne banke u Senti sa kojom Javno komunalno-stambeno preduzeće Senta ima zaključen ugovor o zakupu sefa.

Ispravnost kopija-arhiva proverava se najmanje na šest meseci 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.

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

Član 22.

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

Svakog poslednjeg radnog dana u nedelji datoteke u kojima se nalazi dnevnik aktivnosti se arhiviraju po proceduri za izradu kopija-arhiva ostalih podataka u IKT sistemu, u skladu sa čl. 20 ovog pravilnika.

18. Obezbeđivanje integriteta softvera i operativnih sistema

Član 23.

U IKT sistemu može da se instalira samo softver za koji postoji važeća licenca u vlasništvu Javnog komunalno-stambenog preduzeća Senta, odnosno Freeware i Opensource verzije.

Instalaciju i podešavanje softvera može da vrši samo P-R sektor, 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.

19. Zaštita od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema

Član 24.

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

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

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

Član 25.

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 načelnika Uprave.

21. Zaštita podataka u komunikacionim mrežama uključujući uređaje i vodove

Član 26.

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.

P-R sektor je dužan da stalno vrši kontrolni pregled mrežne opreme i blagovremeno preduzima mere u cilju otklanjanja eventualnih nepravilnosti.

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

Član 27.

Razmena podataka sa organima i organizacijama se vrši u skladu sa unapred zaključenim ugovorom/protokolom.

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

Član 28.

Način instaliranja novih, zamena i održavanje postojećih resursa IKT sistema od strane trećih lica koja nisu zaposlena u Jvnom komunalno-stambenom preduzeću Senta, biće definisan ugovorom koji će biti sklopljen sa tim licima.

P-R sektor je zadužen za tehnički nadzor nad realizacijom ugovorenih obaveza od strane trećih lica.

O uspostavljanju novog IKT sistema, odnosno uvođenju novih delova i izmenama postojećih delova IKT sistema P-R sektor vodi dokumentaciju.

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

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

Član 29.

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

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

Član 30.

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.

P-R sektor je odgovoran za kontrolu pristupa i nadzor nad izvršenjem ugovorenih obaveza, kao i za poštovanje odredbi ovog pravilnika kojima su takve aktivnosti definisane.

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

Član 31.

P-R sektor je odgovoran za nadzor nad poštovanjem ugovorenih obaveza od strane trećih lica-pružaoca usluga, posebno u oblasti poštovanja odredbi kojima je definisana bezbednost resursa IKT sistema. U slučaju nepoštovanja ugovorenih obaveza P-R sektor je dužan da odmah obavesti direktora, kako bi on mogao da preduzme mere u cilju otklanjanja nepravilnosti.

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

Član 32.

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

Po prijemu prijave P-R sektor je dužan da odmah obavesti direktora i preduzme mere u cilju zaštite resursa IKT sistema.

Ukoliko se radi o incidentu koji je definisan u skladu sa Uredbom o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u informaciono-komunikacionim sistemima od posebnog značaja, P-R sektor je dužan da pored direktora obavesti i nadležni organ definisan ovom uredbom.

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

28. Mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima

Član 33.

U slučaju vanrednih okolnosti, koje mogu da dovedu do izmeštanja IKT sistema iz zgrade Javnog komunalno-stambenog preduzeća Senta, P-R sektor je dužan da u najkraćem roku prenese delove IKT sistema (ili obezbedi 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.

Specifikaciju delova IKT sistema koji su neophodni za funkcionisanje u vanrednim situacijama izrađuje P-R sektor, i to u tri primerka, od kojih se jedan nalazi kod njega, drugi kod zaposlenog nadležnog za poslove odbrane i vanredne situacije, a treći primerak kod direktora.

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.

III. Izmena Pravilnika o bezbednosti

Član 34.

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, P-R sektor je dužan da obavesti direktora, kako bi on mogao da pristupi izmeni ovog pravilnika, u cilju unapređenje mera zaštite, načina i procedura postizanja i održavanja adekvatnog nivoa bezbednosti IKT sistema, kao i preispitivanje ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema.

IV. Provera IKT sistema

Član 35.

Proveru IKT sistema vrši P-R sektor.

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

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

V.Sadržaj izveštaja o proveri IKT sistema

Član 36.

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

VI. Prelazne i završne odredbe

Član 37.

Ovaj pravilnik stupa na snagu danom objavljivanja na oglasnoj tabli/internet stranici Javnog komunalno- stambenog preduzeća Senta.

Broj: 01-995-09/2021
Datum: 05.07.2021.

V. d. Direktora

Akoš Slavnić, dipl.ekon.