Temeljem članka 24. Zakona o informacijskoj sigurnosti (NN RH 79/07) te članka 43. Statuta Grada Čakovca (Sl. gl. Grada Čakovca broj 9/09) i članka 8. Poslovnika gradonačelnikovog stručnog kolegija (Sl. gl. Grada Čakovca 10/09), gradonačelnik Grada Čakovca, je na svom 28. stručnom kolegiju, održanom dana 14. ožujka 2013. godine, donio

P R A V I L N I K
o sigurnosti Informacijskog sustava Grada Čakovca

I. OPĆE ODREDBE

Članak 1.

Ovim se Pravilnikom utvrđuju:

- ciljevi zaštite sigurnosti Informacijskog sustava (u daljnjem tekstu: IS) Grada Čakovca,
- organizacija zaštite sigurnosti,
- mjere i sredstva zaštite sigurnosti,
- provedba mjera i sredstava zaštite sigurnosti,
- odgovornost zbog nepridržavanja mjera i sredstava zaštite sigurnosti,
- završne odredbe.

Članak 2.

Pojedini pojmovi koji se koriste u ovom Pravilniku imaju sljedeće značenje:

1. **Administrator** - autorizirani korisnik sa specijalnim ovlastima za rad sa računalom, računalnim programima, bazama podataka, s ovlastima pristupa do računala kao samostalne radne jedinice ili kao jedinice na mreži, a za potrebe administriranja i nadzora nad bazama podataka te administriranja, nadzora i upravljanja računalnom i mrežnom opremom.
2. **Aplikacija** - aplikacija je program ili skup programa dizajniranih za pružanje podrške poslovnom procesu.
3. **Autentifikacija podataka** - postupak kod kojega se ispituje da li je korisnik (njegova poruka) autentična, tj. da li se radi upravo o poruci koja se očekuje. Potvrda da nitko nije nešto dodavao u poruku niti mijenjao poruku. Postupak je takav da se na strani pošiljatelja dodaje dodatna informacija poruci koja ovisi o sadržaju poruke, a na prijemnoj strani se to verificira.
4. **Autorizacija** - postupak kod kojega najčešće programska podrška ispituje da li je oprema ili korisnik koji pristupa autoriziran, tj. da li mu je dozvoljen pristup.
5. **Autorizirani korisnik** - korisnik koji je uspješno autorizirao.
6. **Dekriptiranje podataka** - proces kod kojega se kodirani tekst vraća u prvobitno originalno stanje.
7. **Digitalni certifikat** - znači potvrdu u elektroničkom obliku koji povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe. Certifikat je, u smislu Zakona o elektroničkom potpisu, svaka elektronička potvrda kojom se potvrđuje identitet potpisnika u postupcima razmjene elektroničkih zapisa. Kvalificirani certifikat je svaka elektronička potvrda kojom davatelj usluga izdavanja kvalificiranih certifikata potvrđuje napredni elektronički potpis.
8. **Elektronička pošta** - protokol na Internetu, koji omogućuje korisnicima slanje tekstualnih poruka s računala na računalo. Kao dodatak tekstualnoj poruci mogu se

poslati sve vrste dokumenata u elektronskom formatu: fotografije, filmovi, animacije, dokumenti itd.

9. **Elektronički zapis** - je cjelovit skup podataka koji su elektronički generirani, poslani, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju. Sadržaj elektroničkog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor te računalne baze podataka.
10. **Elektronički potpis** - znači skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnost potpisanog elektroničkog dokumenta.
11. **Enkripcija podataka** - postupak pretvaranja čitljivih podataka u nečitljive
12. **IS** – informacijski sustav je formalni dio komunikacijskog sustava određene poslovne jedinice, a sastoji se od skupine ljudi i strojeva koji obrađuju informacije i nalaze se u komunikacijskoj vezi radi realizacije poslovnih ciljeva.
13. **Korisnički račun** - mrežno ime ili identitet korisnika koji radi na računalu priključenom na mrežu računala.
14. **Korisnik** - korisnik informacijskog sustava je osoba koja koristi računalnu opremu, računalne programe i baze podataka, koja razvija programe i aplikacije za podršku poslovnom procesu, koja kreira, organizira i održava baze podataka te koja koristi računalo kao samostalnu radnu stanicu ili kao radnu stanicu na mreži.
15. **Kriptiranje podataka** - postupak kod kojega se osigurava tajnost podataka korištenjem algoritma za kriptiranje. Samo željeni korisnik na prijemnoj strani koji ima odgovarajući binarni broj koji se naziva ključ može dekriptirati podatke i doći do originalnog teksta.
16. **Kriptografija** - matematički algoritmi i procesi kojima se dobivaju nečitljive poruke, kao i konverzija tih poruka u čitljivi tekst.
17. **Klijent** - klijent je računalo koje otvara i koristi programe i aplikacije sa servera ili preuzima s njega programe i podatke.
18. **Lozinka** - jedinstveni red znakova koje zna samo korisnik.
19. **Napredan elektronički potpis** - znači elektronički potpis koji pouzdano jamči identitet potpisnika i koji je povezan isključivo s potpisnikom, nedvojbeno identificira potpisnika, nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika te sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka. Napredan elektronički potpis ima istu pravnu snagu i zamjenjuje vlastoručni potpis, odnosno vlastoručni potpis i otisak pečata ako je izrađen u skladu s odredbama Zakona o elektroničkom potpisu.
20. **Softver** - softver ili programska podrška za rad računala je niz instrukcija i podataka pohranjenih u elektroničkom obliku u računalu.
21. **Upravni odjel za Upravu** – u daljnjem tekstu „Odjel“ je gradski odjel u čijem je djelokrugu upravljanje Informacijskim sustavom Grada Čakovca.
22. **Operacijski sustav** - operacijski sustav je skup osnovnih programa i alata koji pokreću računalo, upravljaju svim procesima u računalu, fizičkim i programskim dijelovima računala te uređuju njihovu komunikaciju.
23. **Mreža** - mrežna infrastruktura za podršku informacijskom sustavu obuhvaća sve mrežne poslužitelje (poslužitelje baza podataka, web poslužitelje, poslužitelje za administriranje i nadzor mreže, za primanje i slanje elektroničke pošte, ...), radne stanice s pripadajućom perifernom opremom, mrežnu i komunikacijsku opremu za povezivanje lokalnih radnih stanica u lokalne mreže i izdvojenih, dislociranih radnih stanica kojima se omogućuje pristup do zajednički baza podataka.
24. **Radna stanica** - računalo s pripadajućom perifernom opremom na kojem korisnik koristi računalne programe i baze podataka, razvija programe i aplikacije za podršku poslovnom procesu, kreira, organizira i održava baze podataka, bez obzira da li ga koristi kao samostalnu radnu stanicu ili kao radnu stanicu na mreži.

25. **Poslužitelji** - poslužitelji su računala ili programski paketi koji omogućavaju specifičnu vrstu usluge za klijent programe koji se vrte na drugim računalima.
26. **Virus** - kompjuterski virusi su kratki programi, čija je odlika brzo razmnožavanje, odnosno multipliciranje i izvršavanje određenih primarnih komandi, a virusi novije generacije prilikom kopiranja još i mutiraju, mijenjajući svoj osnovni kod, odnosno rade štetu u sistemu.
27. **Vatrozid** - sigurnosna zaštita, filter koji ograničava pristup/prolaz neautoriziranim korisnicima za zaštitu lokalne mreže od neovlaštenog pristupa iz vanjskog svijeta te za sprečavanje nedozvoljenog prometa mrežom iznutra prema van.
28. **VPS** – Virtualni server koje se nalazi u podatkovnim centrima.

II. CILJEVI ZAŠTITE SIGURNOSTI IS-a

Članak 3.

Ciljevi zaštite sigurnosti IS-a u smislu ovoga Pravilnika su:

- očuvanje i zaštita integriteta IS-a Grada Čakovca,
- reguliranje dostupnosti podacima,
- zaštita povjerljivosti podataka, i
- čuvanje poslovne tajne.

Članak 4.

IS Grada Čakovca potrebno je štititi od:

- elementarnih nepogoda,
- požara,
- prekida ili neurednog napajanja električnom energijom,
- neovlaštenog pristupa i korištenja podataka i/ili programa,
- krađe opreme,
- krađe podataka i/ili programa,
- namjernog uništenja opreme i/ili podataka i/ili programa,
- zaraze računalnim virusom,
- neovlaštenog korištenja resursa,
- sprečavanja drugih u korištenju resursa,
- slučajnog gubitka podataka i/ili programa,
- kvara opreme.

Otklanjanje opasnosti iz stavka 1. ovoga članka osigurava se utvrđivanjem organizacije zaštite sigurnosti, mjera i sredstva zaštite sigurnosti, provedbe mjera i sredstava zaštite sigurnosti te utvrđivanja odgovornosti zbog nepridržavanja mjera i sredstava zaštite sigurnosti.

Članak 5.

IS Grada Čakovca, u smislu ovoga Pravilnika, obuhvaća informacijske sustave gradske uprave na svim lokacijama i zajedničke baze podataka IS-a Grada Čakovca i informacijskih sustava trgovačkih društava i ustanova u vlasništvu/suvlasništvu Grada Čakovca postavljene na središnjem mrežnom poslužitelju.

Očuvanje i zaštitu integriteta IS-a Grad Čakovec osigurava primjenom ovoga Pravilnika nad svim informacijskim sustavima i bazama podataka iz stavka 1. ovoga članka.

Članak 6.

Dostupnost podacima IS-a Grada Čakovca utvrđuje se organizacijom, mjerama i sredstvima zaštite sigurnosti utvrđenim ovim Pravilnikom.

Podaci, u smislu ovoga Pravilnika, su elektronički zapisi, dokumenti, njihovi sadržaji i prilozi, kao i usmena priopćenja i informacije povjerljive naravi, iznijeti u radu odjela gradske uprave Grada Čakovca te trgovačkih društava i ustanova u vlasništvu/suvlasništvu Grada Čakovca.

Dokumenti, u smislu ovoga Pravilnika, su svi pisani sastavci (akti, tablice, grafikoni, nacrti, crteži, i slično).

Članak 7.

Tajna je podatak koji je zakonom, drugim propisom ili općim aktom Grada Čakovca određen kao tajni.

Podaci iz stavka 1. ovoga članka smatraju se tajnim bez obzira jesu li napisani rukom, osobnim računalom, strojem, tiskani, stenografirani, šifrirani, filmirani, fotokopirani, snimljeni na magnetnoj vrpci, disketi i drugim magnetnim medijima.

Prije usmenog priopćavanja tajnih podataka daje se prethodno upozorenje o tajnosti koje ima istu važnost kao i pisano utvrđena vrsta tajne i stupanj tajnosti.

Poslovnu tajnu predstavljaju podaci koji su kao poslovna tajna određeni zakonom, drugim propisom ili općim aktom Grada Čakovca.

Članak 8.

Tajne podatke su dužni čuvati svi dužnosnici i djelatnici Grada Čakovca, zaposleni u trgovačkim društvima i ustanovama u vlasništvu/suvlasništvu Grada Čakovca koji imaju pristup podacima iz članka 7. ovoga Pravilnika.

Dužnost čuvanja tajnih podataka odnosi se na sve osobe iz prethodnog stavka ovoga članka i nakon isteka njihova mandata, prestanka radnog odnosa ili prestanka obavljanja poslova.

Članak 9.

Za neovlašteno priopćavanje tajnih podataka u smislu odredaba ovoga Pravilnika Grad Čakovec će postupiti u skladu sa Zakonom i općim aktom Grada Čakovca kojim se uređuje zaštita tajnosti podataka.

III. ORGANIZACIJA ZAŠTITE SIGURNOSTI

1. Područje obuhvata zaštite

Članak 10.

Organizacijom zaštite sigurnosti, u smislu ovoga Pravilnika, obuhvaćeni su:

- zgrade,
- prostorije,
- mrežna infrastruktura,
- poslužitelji,
- radne stanice,
- operacijski sustavi,
- aplikacije,
- podaci i baze podataka i
- neumreženi sustavi IS-a Grada Čakovca.

Članak 11.

Mjere i sredstva zaštite sigurnosti IS-a Grada Čakovca utvrđene ovim Pravilnikom primjenjuju se nad svim objektima iz članka 10. ovoga Pravilnika.

2. Načini korištenja IS-a

Članak 12.

Osobna računala, samostojeća ili povezana u lokalne mreže, s pripadajućim programima i podacima, kao i ostala informatička oprema smiju se koristiti isključivo za potrebe posla i u okviru ovlaštenja za obavljanje poslova.

Zabranjeno je koristiti osobna računala i ostalu informatičku opremu, aplikacije i podatke izvan objekata Gradske uprave ili službenih prostorija bez pisanog naloga ovlaštene osobe.

Članak 13.

Korisnici informatičke opreme dužni su pridržavati se pravila za korištenje informatičke opreme i provoditi sve predviđene procedure i tehničke upute za korištenje informatičke opreme.

Članak 14.

Tehničke zahvate na informatičkoj opremi (promjena konfiguracije, zamjena pojedinih dijelova opreme) smiju obavljati samo za to ovlaštene osobe za informatičke poslove ili ovlašteni serviseri uz nadzor djelatnika Odjela, uz pisani nalog.

Korisnicima informatičke opreme je zabranjeno obavljati tehničke zahvate iz prethodnog stavka ovoga članka.

Članak 15.

Korisnik smije koristiti samo odgovarajući potrošni materijal (optički mediji, magnetski mediji, trake, tonere, tinte za pisače i slično) i poštivati propisane procedure kod nabave i zamjene kako ne bi nastale štete na informatičkoj opremi.

Procedure iz prethodnog stavka ovoga članka propisuju osobe iz Odjela zadužene za obavljanje informatičkih poslova Grada Čakovca.

3. Ažurna evidencija svih računalnih i mrežnih resursa

Članak 16.

Osobe zadužene za informatičke poslove Grada Čakovca nadležne su za vođenje ažurne evidencije o računalnim i mrežnim resursima IS-a Grada Čakovca.

Svako premještanje računala ili njihovih perifernih uređaja s jedne lokacije na drugu odobrava, izvodi i evidentira ovlaštena osoba Odjela.

Zastarjela oprema može se zamijeniti ili staviti izvan upotrebe samo od strane ovlaštene osobe za informatičke poslove Grada Čakovca.

Članak 17.

Premještanje računala i zamjenu zastarjele opreme izvodi ovlaštena osoba Odjela.

4. Korisnici IS-a

Članak 18.

Korisnik IS-a Grada Čakovca je svaka osoba koja koristi računalnu opremu, računalne programe i baze podataka, koja razvija programe i aplikacije za podršku poslovnom procesu, koja kreira, organizira i održava baze podataka te koristi računalo kao samostalnu radnu stanicu ili kao radnu stanicu na mreži.

Osobe zadužene za informatičke poslove Grada Čakovca dužne su voditi evidenciju o korisnicima IS-a Grada Čakovca.

Članak 19.

Korisnicima IS-a Grada Čakovca iz članka 18. ovoga Pravilnika osobe zadužene za informatičke poslove Odjela dodjeljuje ovlasti za korištenje IS-a primjereno zahtjevima posla kojeg obavljaju.

5. Administratori IS-a

Članak 20.

Administrator IS-a Grada Čakovca je autorizirani korisnik sa specijalnim ovlastima za rad sa računalom, računalnim programima, bazama podataka, s ovlastima pristupa do računala kao samostalne radne jedinice ili kao jedinice na mreži, a za potrebe administriranja

i nadzora nad bazama podataka te administriranja, nadzora i upravljanja računalnom i mrežnom opremom.

Viši informatički savjetnik Grada Čakovca je dužan voditi evidenciju o administratorima IS-a Grada Čakovca.

Članak 21.

Administratoru IS-a Grada Čakovca iz članka 20. ovoga Pravilnika Odjel dodjeljuje ovlasti za korištenje IS-a primjereno zahtjevima posla kojeg obavlja.

6. Instalacija strojne i programske opreme

Članak 22.

Sva nabava i instalacija strojne i programske informatičke opreme obavlja se isključivo uz odobrenje osobe zadužene za informatičke poslove Odjela Grada Čakovca.

Odjel propisuje tehničke i radne karakteristike koje treba zadovoljiti informatička oprema i standardni uvjeti okoline sa stanovišta sigurnosti, gdje se ona instalira.

Članak 23.

Instaliranje novih programa i izmjene postojećih programa smiju obavljati samo za to ovlaštene osobe Odjela ili ovlašteni serviseri uz nadzor djelatnika Odjela, uz pisani nalog.

Na poslužitelje ili osobna računala smije se instalirati samo programska podrška i podaci koje odobri ili nabavi Odjel.

7. Održavanje sustava od strane vanjskih organizacija

Članak 24.

Održavanje sustava od strane drugih pravnih osoba provodi se uz odobrenje Odjela.

Svaka osoba koja po bilo kojoj osnovi obavlja u Gradu Čakovcu privremene ili povremene poslove, ili poslove temeljem posebnog ugovora, dužna je pridržavati se odredaba ovoga Pravilnika. Zaposleni u pravnim osobama koji obavljaju određene poslove za Grad Čakovec, za vrijeme obavljanja tih poslova, dužni su provoditi mjere zaštite sigurnosti utvrđene ovim Pravilnikom.

Komunalna i trgovačka društva i ustanove u vlasništvu/suvlasništvu Grada Čakovca koja koriste resurse IS-a Grada Čakovca dužna su provoditi mjere zaštite sigurnosti utvrđene ovim Pravilnikom.

Članak 25.

Odjel je dužan upoznati osobe navedene u članku 24. s odredbama ovoga Pravilnika pri davanju odobrenja za korištenje resursa IS-a Grada Čakovca.

8. Priključivanje i isključivanje poslužitelja i radnih stanica na mrežu

Članak 26.

Korisnicima je zabranjeno priključivanje i isključivanje poslužitelja i radnih stanica na lokalnu mrežu bez ovlaštenja Odjela.

9. Rad na daljinu (teleworking)

Članak 27.

Bez prethodnog odobrenja Odjela korisnicima je zabranjeno:

povezivanje osobnih računala na Internet ili na neku drugu mrežu ili komunikacijski priključak izvan IS-a Grada Čakovca,
spajanje računala izvan IS-a Grada Čakovca na računala i računalne sustave Grada Čakovca.

Članak 28.

O svim uočenim nepravilnostima u radu i korištenju informatičke opreme djelatnik Grada Čakovca je dužan odmah izvijestiti nadležnu osobu Odjela ili osobu odgovornu za provedbu mjera zaštite sigurnosti i provedbu sigurnosne politike.

IV. MJERE I SREDSTVA ZAŠTITE SIGURNOSTI

Članak 29.

Prijetnje IS-u Grada Čakovca imaju za posljedicu smanjenje resursa, ograničavanje resursa, privremeni prestanak rada IS-a, gubitak podataka, gubitak programa i podataka ili potpuni gubitak IS-a.

1. Pristupna prava korisnika

Članak 30.

Dodjela pristupnih prava korisnika provodi se s ciljem omogućavanja ispravnog korištenja programa, podataka i resursa IS-a Grada Čakovca.

Radi provođenja mjere dodjele pristupnih prava korisnicima mreže, aplikacija i baza podataka IS-a Grada Čakovca pohranjenih u računalima, potrebno je provoditi sljedeće radnje:

Odjel je dužan organizirati i provjeravati autentičnost korisnika koji pristupaju mreži računalnih sustava,
Odjel je dužan organizirati pristup i provesti kontrolu pristupa svim računalnim sustavima Grada Čakovca samo ovlaštenim djelatnicima primjereno zahtjevima posla kojeg obavljaju,
Odjel je dužan omogućiti uređaje i softver za autentifikaciju za korisnike koji imaju velika ovlaštenja pristupa mreži i podacima,
Odjel je dužan provesti sve nadopune, brisanja i promjene u organizaciji i kontroli pristupa računalnim sustavima u skladu s odobrenim zahtjevom krajnjeg korisnika,

Odjel je dužan voditi i održavati ažurnim popis administrativnih pristupnih kodova i lozinki te čuvati taj popis na sigurnom mjestu,
Odjel je dužan onemogućiti anonimni pristup bilo koje vrste do radnih stanica,
Odjel je dužan kontrolirati ADSL i slične priključke na mrežu a instalaciju novih mrežnih uređaja odobrava Odjel,
Odjel je dužan pratiti sva događanja na mreži,
korisnik računalnog sustava je odgovoran za sve računalne transakcije izvršene uz uporabu njegove korisničke identifikacije i lozinke,
zabranjeno je obznanjivati lozinke drugima te se lozinka mora promptno promijeniti ako postoji sumnja da je postala poznata drugima,
zabranjeno je pohranjivati lozinku na mjesto gdje je do nje lako doći,
lozinka se mora mijenjati u roku ne dužem od 90 dana,
ne smiju se koristiti lozinke koje se mogu lako pamtiti, lako odgonetnuti ili probiti od strane drugih,
lozinke moraju sadržavati najmanje osam znakova i to kombinaciju slova, brojki i simbola,
korisnik mora odjaviti svoj korisnički račun kada prestaje s radom na računalu na duže vrijeme,
kadrovska služba Grada Čakovca je dužna promptno Odjel o tome da li nekom djelatniku prestaje radni odnos u Gradu Čakovcu ili se raspoređuje na rad u drugi odjel gradske uprave, kako bi se mogla opozvati njegova ovlaštenja za pristup resursima,
radna stanica se mora ugasiti kada nije u upotrebi (npr. preko noći).

2. Vatrozid

Članak 31.

Vatrozid se primjenjuje s ciljem organizacije i kontrole prometa mrežom te sprječavanja nedozvoljenog prometa mrežom.

Radi provođenja mjera organizacije, kontrole i zaštite prometa mrežom potrebno je provoditi sljedeće radnje:

Odjel je dužan primijeniti vatrozid za organizaciju i kontrolu prometa podacima između vanjskog svijeta i unutrašnjeg dijela mreže,
Odjel je dužan primijeniti vatrozid za sprječavanje nedozvoljenog prometa mrežom iznutra prema van,
Odjel je dužan primijeniti vatrozid za sprječavanje nedozvoljenog prometa mrežom iz vanjskog svijeta prema unutrašnjem dijelu mreže,
Odjel je dužan primijeniti vatrozid za sprečavanje nedozvoljenog prometa zaštićenim segmentom lokalne mreže od ostale lokalne mreže.

3. Kriptiranje, digitalni certifikati i digitalni potpis

Članak 32.

Kriptiranje, digitalni certifikati i digitalni potpis provode se u cilju sprečavanja slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenih izmjena podataka i/ili programa, neovlaštenog korištenja resursa, sprečavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Radi provođenja mjere zaštite povjerljivosti i integriteta podataka potrebno je provoditi sljedeće radnje:

Odjel je dužan omogućiti korisnicima korištenje računalne opreme ili programa za izradu i verificiranje elektroničkog potpisa za identifikaciju potpisnika i vjerodostojnost potpisanog elektroničkog dokumenta,
Odjel je dužan osigurati davatelja usluga certificiranja koji izdaje elektroničku potvrdu kojom se potvrđuje identitet potpisnika u postupcima razmjene elektroničkog zapisa (certifikat) za sigurnu provedbu usluga certificiranja,
za čuvanje povjerljivih i tajnih podataka korisnik je dužan koristiti programe za kriptiranje podataka spremljenih na radnim stanicama,
pri slanju povjerljivih i tajnih podataka elektroničkom poštom pošiljatelj je dužan koristiti mail program koji podržava kriptiranje poruka,
korisnik elektroničkog potpisa je dužan koristiti elektronički potpis u skladu sa propisima kojima se uređuje elektronički potpis.

4. Internet i elektronička pošta

Članak 33.

Sigurno korištenje Interneta i elektroničke pošte provodi se u cilju sprečavanja zaraze računalnim virusom, slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprečavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Radi sigurnog korištenja Interneta i elektroničke pošte potrebno je provoditi sljedeće radnje:

dozvoljena je komunikacija putem Interneta koja se obavlja iz profesionalnih razloga i koja ne utječe negativno na produktivnost,
dozvoljeno je korištenje web preglednika za prikupljanje poslovnih informacija s komercijalnih web adresa,
dozvoljeno je korištenje Interneta za pristup bazama podataka radi pronalaženja poslovnih informacija,
dozvoljeno je korištenje elektroničke pošte u svrhu ostvarivanja poslovnih kontakata,
obavezno je čuvanje elektroničke pošte koja je značajna za poslovni proces,
korisnik Interneta i elektroničke pošte snosi odgovornost za sadržaj svih tekstova, zvučnih zapisa ili slika koje objavljuje ili šalje putem Interneta,
uz svaku komunikaciju putem Interneta mora biti naznačeno ime djelatnika koji je obavlja,
zabranjeno je slanje i prosljeđivanje lančane elektroničke pošte, tj. poruka koje uključuju naputke za prosljeđivanje poruka drugima,
zabranjeno je slanje iste poruke na više od deset (10) prijamnih adresa ili na više od jedne dostavne (distribucijske) liste koja nije poslovnog sadržaja,
zabranjeno je obavljanje privatnih i osobnih poslova uz korištenje resursa IS-a Grada Čakovca,
zabranjeno je slanje bilo kakvog sadržaja koji je ofanzivan, koji primatelju može stvoriti neprilike ili štetu, ili je obmanjujući,
protuvirusna zaštita mora biti obavezno aktivirana kod prijama elektroničke pošte i pridruženih datoteka,

zabranjeno je pokretanje izvršnih datoteka ako se ne zna o čemu se radi i da li je izvor pouzdan.

5. Protuvirusna zaštita

Članak 34.

Protuvirusna zaštita provodi se u cilju sprečavanja zaraze računalnim virusom, slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprečavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Radi provođenja protuvirusne zaštite potrebno je provoditi sljedeće radnje:

Odjel je dužan instalirati i održavati protuvirusne programe na svim poslužiteljima i radnim stanicama Grada Čakovca redovitim ažuriranjem u pogledu novih vrsta virusa,
Odjel je dužan konfigurirati protuvirusni program tako da vrši protuvirusno skeniranje svih ulaznih objekata,
Odjel je dužan odgovoriti na sve napade računalnih virusa, uništiti svaki otkriveni virus te dokumentirati svaki incident,
zabranjeno je namjerno unositi računalne viruse u računala Grada Čakovca,
svatko tko sumnja da je njegovo računalo zaraženo virusom mora odmah isključiti računalo i o tome obavijestiti odgovornu osobu za provedbu mjera zaštite sigurnosti.

6. Korištenje softvera

Članak 35.

Sigurno korištenje softvera provodi se u cilju sprečavanja zaraze računalnim virusom, slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprečavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Radi provođenja zaštite softvera potrebno je provoditi sljedeće radnje:

pridržavati se odredbi Zakona o autorskom pravu i srodnim pravima,
pridržavati se licencnih ugovora o korištenju autorski zaštićenog softvera,
Odjel je dužan voditi evidenciju o svim licencama softvera u posjedu Grada Čakovca,
Odjel je dužan periodično, a najmanje dva puta godišnje, izvršiti uvid u računala u posjedu Grada Čakovca kako bi verificirao da je instaliran samo softver za čije korištenje je Grad Čakovec ovlašten,
samo licencirani softver i softver u vlasništvu Grada Čakovca smije se instalirati na računalima Grada Čakovca,
zabranjena je instalacija bilo kakvog softvera za koji se nema dozvola Odjela,
zabranjena je izmjena bilo kakvog softvera za koju se nema dozvola Odjela,
zabranjena je deinstalacija bilo kojeg softvera instaliranog na računalu bez dozvole Odjela.

7. Zaštita podataka

Članak 36.

Zaštita podataka provodi se u cilju sprečavanja zaraze računalnim virusom, slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprečavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Radi provođenja zaštite podataka potrebno je provoditi sljedeće radnje:

magnetni mediji s podacima se moraju pohranjivati pod ključem,
magnetne medije treba pohranjivati na mjestima na kojima nisu izloženi vanjskim rizicima, kao što su toplina, izravna sunčeva svjetlost i magnetska polja, Odjel je dužan svakodnevno pohranjivati korisničke podatke sa poslužitelja na odvojene magnetne medije i čuvati ih u vodootpornim i vatrootpornim ormarima udaljeno od poslužitelja, uz obaveznu provjeru kvalitete izrađenih kopija probnim čitanjem,
Odjel je dužan nakon svake instalacije ili modifikacije sistemskih datoteka pohraniti sistemski softver i sistemske podatke sa poslužitelja na odvojene magnetne medije i čuvati ih u vodootpornim i vatrootpornim ormarima udaljeno od poslužitelja,
Odjel je dužan samostalne radne stanice koje nemaju ugrađenu jedinicu za pohranjivanje podataka na drugi magnetni medij spojiti na mrežu kako bi se omogućila automatizirana centralizirana zaštita podataka preko mreže,
svi poslovni podaci po instaliranju diskovnog podsistema pohranjuju se na diskovni podsistem i osiguravaju se od strane Odjela.
Odjel je dužan sve korisničke podatke čuvati na odvojenoj lokaciji, VPS ili *Cloud* rješenjima, sa odgovarajućom enkripcijom kod prijenosa podataka.

8. Fizička zaštita prostorija s opremom

Članak 37.

Fizička zaštita prostorija s opremom provodi se u cilju sprečavanja kvara opreme, krađe opreme, prekida ili neurednog napajanja električnom energijom, požara ili elementarnih nepogoda, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprečavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

Radi provođenja fizičke zaštite prostorija s opremom potrebno je provoditi sljedeće radnje:

poslužitelji i aktivna mrežna oprema se moraju smjestiti u sigurnim i čvrstim prostorijama koje nisu izložene poplavi,
poslužitelji i mrežna oprema se moraju štititi stalnim izvorom energije (UPS), a ostala računalna oprema štiti se od strujnih udara stabilizatorima napona,
prostorije s poslužiteljima se moraju štititi od visoke ili niske vlažnosti zraka te ekstremne topline ili hladnoće klimatizacijskim uređajima,
prostorije s računalnom opremom moraju biti zaštićene od požara u skladu s Zakonom o zaštiti od požara
prostorija s glavnim komunikacijskim čvorom i telefonskom centralom mora biti zaključana i pristup dozvoljen samo uz prisustvo ovlaštene osobe,

u trenucima kada nitko ne boravi u prostorijama s računalnom opremom, vrata moraju biti zaključavana, a prozori zatvarani,
u slučaju krađe ili gubitka ključa od prostorije s računalnom opremom treba obavijestiti odgovornu osobu i zamijeniti bravu,
na sva vanjska vrata i prozore mogu biti instalirani uređaji za dojavu nasilnog ulaza i moraju se redovito kontrolirati,
oprema koja mora biti smještena na javno pristupnom prostoru mora biti zaštićena, a javni pristup nadziran,
portiri, odnosno čuvari na ulazu u zgradu moraju pratiti kretanje svih osoba na ulazu,
nepoznate osobe moraju pružiti dokaze o svojem identitetu,
prije dozvole ulaska posjetitelju potrebno je verificirati posjetu kod osobe kojoj se posjetitelj upućuje,
portiri, odnosno čuvari na ulazu u zgradu moraju voditi evidenciju o datumu i vremenu ulaza i izlaza posjetitelja,
pristup do uređaja za obradu podataka mora biti kontroliran i dozvoljen samo ovlaštenim osobama,
područje na kojem se obavlja isporuka i preuzimanje opreme ili potrošnog materijala mora biti kontrolirano i po mogućnosti odvojeno od područja gdje se nalaze sredstva za obradu podataka.

V. PROVEDBA MJERA I SREDSTAVA ZAŠTITE SIGURNOSTI

1. Načini provedbe

Članak 38.

Poduzimanje i provođenje propisanih mjera i sredstava zaštite sigurnosti IS-a Grada Čakovca provodi se u skladu s odredbama ovoga Pravilnika.

Članak 39.

Odjel neposredno organizira i nadzire provođenje mjera i sredstava zaštite sigurnosti utvrđenih ovim Pravilnikom.

U cilju unapređenja zaštite sigurnosti IS-a odgovorna osoba za provedbu mjera i sredstava zaštite sigurnosti predlaže, osim mjera i sredstava utvrđenih ovim Pravilnikom, provedbu drugih mjera zaštite sigurnosti u skladu sa zakonom i opće prihvaćenim pravilima struke.

Članak 40.

Odgovorna osoba za provedbu mjera i sredstava zaštite sigurnosti pri obavljanju kontrole i nadzora nad provedbom mjera zaštite sigurnosti dužna je izvijestiti neposrednog rukovoditelja kod kojeg je nadzor obavljen o rezultatima kontrole i unijeti ih u redovna izvješća.

Ako odgovorna osoba za provedbu mjera zaštite sigurnosti pristupa rješavanju složenijih problema s područja zaštite sigurnosti IS-a surađivat će sa svim stručnim službama u tijelima gradske uprave Grada Čakovca.

Članak 41.

Odgovorna osoba za provedbu mjera zaštite sigurnosti obavlja sljedeće poslove:

obavlja redovitu kontrolu provedbe mjera zaštite sigurnosti utvrđenih ovim Pravilnikom,
surađuje i koordinira rad na izradi uputa za zaštitu sigurnosti IS-a,
vodi brigu o pravovremenom osposobljavanju djelatnika za zaštitu sigurnosti IS-a te vodi brigu o tome,
izvješćuje Gradonačelnika o utvrđenim nepravilnostima glede sigurnosnih uvjeta i predlaže mjere za otklanjanje istih.

Članak 42.

Prigodom obavljanja kontrole provedbe mjera zaštite sigurnosti IS-a Grada Čakovca propisanih ovim Pravilnikom, odgovorna osoba ima sljedeća ovlaštenja:

narediti prekid obavljanja posla ili radnje kojom se neposredno ugrožava sigurnost IS-a te o tome izvijestiti neposrednog rukovoditelja,
udaljiti s radnog mjesta djelatnika koji svojim postupkom neposredno ugrožava sigurnost IS-a Grada Čakovca te o tome izvijestiti njegovog neposrednog rukovoditelja,
izvijestiti pročelnika pojedinog odjela gradske uprave o neprovođenju propisanih mjera zaštite sigurnosti.

2. Subjekti provedbe

Članak 43.

Svaki djelatnik zaposlen u tijelima gradske uprave Grada Čakovca dužan je poduzimati i provoditi propisane mjere i sredstva zaštite sigurnosti IS-a Grada Čakovca u skladu s ovim Pravilnikom.

Članak 44.

Pročelnici odjela gradske uprave, ravnatelji direkcija i voditelji odsjeka i službi obvezni su:

provoditi i nadzirati provođenje propisanih mjera zaštite sigurnosti,
upoznati novog djelatnika s opasnostima od ugrožavanja sigurnosti IS-a Grada Čakovca,
poduzeti mjere da se nedostaci koji mogu utjecati na sigurnost IS-a, a utvrđeni su pregledom ili prijavljeni od strane odgovorne osobe za provedbu zaštite sigurnosti, odmah uklone,
izvijestiti odgovornu osobu za zaštitu sigurnosti i provođenje mjera zaštite sigurnosti o svakom nastalom problemu ili mogućoj opasnosti za sigurnost IS-a,
udaljiti svakog djelatnika koji pri obavljanju poslova ne provodi i ne primjenjuje mjere zaštite sigurnosti sustava,
provjeriti da li su poduzete potrebne mjere zaštite sigurnosti sustava nakon završetka rada, a prije odlaska iz radnih prostora,
prekinuti rad na radnom mjestu, u tehnološkom procesu, na sredstvu rada i u radnoj okolini ako utvrdi da postoji izravna opasnost za ugrožavanje sigurnosti sustava ili se poslovi izvode suprotno pravilima zaštite.

Članak 45.

Djelatnik zaposlen u tijelima gradske uprave Grada Čakovca dužan je:

upoznati se s odredbama ovog Pravilnika prije stupanja na rad i samostalnog obavljanja poslova na radnom mjestu, kao i svladati osposobljavanje za provedbu mjera zaštite sigurnosti,
poduzimati i provoditi propisane mjere zaštite sigurnosti na radnom mjestu i u radnom prostoru,
svaku uočenu opasnost koja bi mogla biti prijetnja ugrožavanju sigurnosti sustava odmah prijaviti neposrednom rukovoditelju ili osobi odgovornoj za provođenje mjera zaštite sigurnosti.

3. Edukacija korisnika i administratora

Članak 46.

Odgovorna osoba za provedbu mjera i sredstava zaštite sigurnosti dužna je osigurati osposobljavanje djelatnika gradske uprave Grada Čakovca za provedbu mjera i sredstava zaštite propisanih ovim Pravilnikom.

Obveza iz stavka 1 ovoga članka odnosi se i na djelatnike koji su zaposleni na određeno vrijeme, obavljaju stručno osposobljavanje ili su volonteri.

4. Korisnički i administratorski priručnici

Članak 47.

Odgovorna osoba za provedbu mjera i sredstava zaštite sigurnosti dužna je osigurati korisničke i administratorske priručnike.

Korisnički i administratorski priručnici sadrže upute za korisnike i administratore IS-a za korištenje resursa IS-a Grada Čakovca u skladu s odredbama ovoga Pravilnika.

5. Postupanje u incidentnim situacijama

Članak 48.

U slučaju havarije ili incidentne situacije djelatnik Grada Čakovca je dužan odmah izvijestiti odgovornu osobu za provedbu mjera zaštite sigurnosti.

Pod havarijom u smislu ovoga Pravilnika smatra se:

potpuni gubitak sustava,
gubitak programa,
gubitak podataka.

Pod incidentnim situacijama u smislu ovoga Pravilnika smatraju se:

privremeni prestanak rada sustava,
gubitak opreme,

ograničavanje resursa u radu,
smanjenje resursa,
kvar opreme.

6. Nadzor

Članak 49.

Nadzor nad primjenom mjera i sredstava zaštite sigurnosti IS-a Grada Čakovca obavlja se sukladno odredbama ovoga Pravilnika.

Nadzor na primjenom mjera i sredstava zaštite sigurnosti organizira i provodi odgovorna osoba za provedbu mjera i sredstava zaštite sigurnosti.

7. Stalna i povremena revizija

Članak 50.

Odgovorna osoba za provedbu mjera i sredstava zaštite sigurnosti dužna je provoditi stalnu i povremenu reviziju provedbe mjera i sredstava zaštite propisanih ovim Pravilnikom.

VI. ODGOVORNOST ZBOG NEPRIDRŽAVANJA MJERA I SREDSTAVA ZAŠTITE SIGURNOSTI

Članak 51.

Osoba odgovorna za provedbu mjera zaštite sigurnosti i provedbu sigurnosne politike u skladu s ovim Pravilnikom je pročelnik Odjela.

Odgovorna osoba za provedbu mjera zaštite sigurnosti redovito obavlja kontrolu provedbe mjera zaštite utvrđenih ovim Pravilnikom i odgovorna je za provedbu tih mjera.

Članak 52.

Korisnik IS-a Grada Čakovca je dužan pridržavati se svih mjera i sredstava zaštite propisanih ovim Pravilnikom.

Ako korisnik nepridržavanjem odredaba ovoga Pravilnika nanese štetu Gradu Čakovcu, odgovara za pričinjenu štetu sukladno Zakonu i općem aktu Grada Čakovca.

VII. ZAVRŠNE ODREDBE

Članak 53.

Svaki korisnik IS-a dužan je potpisati Izjavu o prihvaćanju sigurnosne politike IS-a Grada Čakovca, u roku od 15 dana od stupanja na snagu ovog Pravilnika (zatečeni korisnici), odnosno od stjecanja statusa korisnika IS-a (budući korisnici).

Obrazac Izjave iz stavka 1. ovoga članka nalazi se u privitku (Prilog 1) i čini sastavni dio ovoga Pravilnika.

Članak 54.

O potpisivanju Izjave iz članka 53. ovoga Pravilnika vodi se očevidnik.

Očevidnik iz prethodnog stavka ovoga članka vodi odgovorna osoba za provedbu mjera zaštite sigurnosti IS-a Grada Čakovca.

Članak 55.

Ovaj Pravilnik stupa na snagu osmoga dana od dana objave u Službenom glasniku Grada Čakovca.

KLASA: 021-05/13-01/42
URBROJ: 2109/02-04-13-02
Čakovec, 14. ožujak 2013.

GRADONAČELNIK
Branko Šalamon

Prilog 1.

I Z J A V A
O PRIHVAĆANJU SIGURNOSNE POLITIKE IS-a

Potpisivanjem ove Izjave izjavljujem da sam:

1. Primio i pročitao Pravilnik o sigurnosti Integralnog Informacijskog sustava Grada Čakovca i razumio ga.

2. Razumio sam i slažem se da svako računalo, softver i memorijski medij koji mi je pribavio Grad Čakovec sadrži vlasništvom zaštićene i povjerljive informacije o Gradu Čakovcu i njenim poslovnim partnerima te da one jesu i ostaju vlasništvo Grada Čakovca u svim svojim dijelovima i trajno.

3. Slažem se da neću kopirati, umnožavati (s izuzetkom sigurnosnog kopiranja), na bilo koji način objavljivati i omogućiti bilo kome drugome da kopira bilo koji dio tih informacija ili softvera.

4. Slažem se da ću, prestankom radnog odnosa u Gradu Čakovcu iz bilo kojeg razloga, odmah vratiti izvorni primjerak i sve kopije svog softvera, računalnog materijala i računalne opreme koje sam primio od Grada Čakovca, a koji su u mome posjedu ili na bilo koji drugi način pod mojom izravnom ili neizravnom kontrolom.

Ime i prezime zaposlenika: _____

Datum: _____

Tijelo gradske uprave:
_____

Potpis zaposlenika: _____