Na osnovu člana 62. Zakona o organizaciji organa uprave u Federaciji Bosne i Hercegovine ("Službene novine FBiH" broj: 35/05), člana 15. Zakona o principima lokalne samouprave u Federaciji Bosne i Hercegovine ("Službene novine FBiH" broj: 49/06), i člana 7. u vezi sa članom 20. Statutarne Odluke o organizaciji Grada Tuzla u skladu sa Zakonom o gradu Tuzla ("Službeni glasnik Grada Tuzla" broj: 1/14 i 3/15), Gradonačelnik Grada Tuzla, donosi

PRAVILNIK
o upotrebi i sigurnosti informacionog sistema Grada Tuzla

I. OPĆE ODREDBE

Član 1.

Ovim se Pravilnikom utvrđuju:

- ciljevi zaštite sigurnosti Informacionog sistema Grada Tuzla,
- organizacija zaštite sigurnosti,
- mjere i sredstva zaštite sigurnosti,
- provođenje mjera i sredstava zaštite sigurnosti,
- odgovornost zbog nepridržavanja mjera i sredstava zaštite sigurnosti,
- završne odredbe.

Član 2.

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

1. 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.

2. Autorizacija - postupak kod kojega najčešće programska podrška (software) ispituje da li je oprema ili korisnik koji pristupa autoriziran, tj. da li mu je dozvoljen pristup.

3. Autorizirani korisnik - korisnik koji je uspješno »prošao« postupak autorizacije, tj. korisnik kojemu je sistem autorizacije dozvolio pristup.

4. Lozinka (password) - jedinstveni red znakova koje zna samo korisnik.

5. Account - mrežno ime ili identitet korisnika koji radi na računaru priključenom na LAN (računarsku mrežu).

6. Korisnik - korisnik informacionog sistema je osoba koja koristi računarsku opremu, računarske programe i baze podataka, koja razvija programe i aplikacije za podršku poslovnom procesu, koja kreira, organizira i održava baze podataka te koja koristi računar kao samostalnu radnu stanicu ili kao radnu stanicu na mreži.

7. Administrator - autorizirani korisnik sa specijalnim ovlastima za rad sa računarom, računarskim programima, bazama podataka, s ovlaštenjima pristupa do računara kao samostalne radne jedinice ili kao jedinice na mreži, a za potrebe administriranja i nadzora nad bazama podataka te administriranja, nadzora i upravljanja računarskom i mrežnom opremom.

8. Firewall - 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.

9. Elektronska pošta (e-mail) - protokol na Internetu, koji omogućuva korisnicima slanje tekstualnih poruka s računara na računar. Kao dodatak tekstualnoj poruci mogu se poslati sve vrste dokumenata u elektronskom formatu: kolor fotografije, animacije, dokumenti itd.

10. Elektronski zapis - je cjelovit skup podataka koji su elektronski generirani, poslati, primljeni ili sačuvani na elektronskom, magnetnom, optičkom ili drugom mediju. Sadržaj elektronskog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, muziku, govor te računarske baze podataka.

11. 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 source, odnosno prave štetu po sistemu.

12. Softver - softver ili programska podrška za rad računara je niz instrukcija i podataka pohranjenih u elektronskom obliku u računaru.

13. Operativni sistem – operativni sistem je skup osnovnih programa i alata koji pokreću računar, upravljaju svim procesima u računaru, fizičkim i programskim dijelovima računara te uređuju njihovu komunikaciju.

14. Aplikacija - aplikacija je program ili skup programa dizajniranih za pružanje podrške poslovnom procesu.

15. Mreža - mrežna infrastruktura za podršku informacionom sistemu obuhvaća sve mrežne servre (servere baza podataka, web servere, servere za administriranje i nadzor mreže, za primanje i slanje elektronske 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.

16. Radna stanica - računar s pripadajućom perifernom opremom na kojem korisnik koristi računarske 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.

17. Serveri - serveri su računari ili programski paketi koji omogućavaju specifičnu vrstu usluge za klijent programe koji se vrte na drugim računarima.

18. Klijent - klijent je računar koji otvara i koristi programe i aplikacije sa servera ili preuzima s njega programe i podatke.

19. Licenca – Pravo ili dozvola za korištenje određenog softvera za određeni vremenski period koji može biti i neograničen. Licencom se pored prava definiše i način i ostali uslovi korištenja softvera.

20. Tajni podatak - činjenica ili sredstvo koje se odnosi na javnu sigurnost, odbranu, vanjske poslove ili obavještajnu i sigurnosnu djelatnost Bosne i Hercegovine, koji je potrebno, u skladu s odredbama Zakona, zaštititi od neovlaštenih osoba i koji je ovlaštena osoba označila oznakom tajnosti.

II. CILJEVI ZAŠTITE SIGURNOSTI IS-a

Član 3.

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

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

Član 4.

IS Grada Tuzla 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 računarskim virusom,
- neovlaštenog korištenja resursa,
- sprečavanja drugih u korištenju resursa,
- slučajnog gubitka podataka i/ili programa,
- kvara opreme.
- drugih okolnosti kojima se može ugroziti IS Grada Tuzla

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

Član 5.

IS Grada Tuzla, u smislu ovoga Pravilnika, obuhvaća informacione sisteme svih službi gradske uprave na svim lokacijama i zajedničke baze podataka IS-a Grada Tuzla i informacionih sistema javnih i drugih ustanova u vlasništvu/suvlasništvu Grada Tuzla ili datih na korištenje organima i institucijama Grada Tuzla a koje su postavljene na mrežnim serverima

Očuvanje i zaštita integriteta IS-a Grada Tuzla osigurava se primjenom ovoga Pravilnika nad svim informacionim sistemima i bazama podataka iz stava 1. ovoga člana.

Član 6.

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

Podaci, u smislu ovoga Pravilnika, su elektronski zapisi, dokumenti, njihovi sadržaji i prilozi, kao i usmena saopštenja i informacije povjerljive naravi, iznijeti u radu službi gradske uprave Grada.

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

Član 7.

Tajni podatak - činjenica ili sredstvo koje se odnosi na javnu sigurnost, odbranu, vanjske poslove ili obavještajnu i sigurnosnu djelatnost Bosne i Hercegovine, koji je potrebno, u skladu s odredbama Zakona, zaštititi od neovlaštenih osoba i koji je ovlaštena osoba označila oznakom tajnosti.

Tajnom se smatra i svaki podatak koji je zakonom, drugim propisom ili općim aktom Grada Tuzla određen kao tajni.

Podaci iz stava 2. ovoga člana smatraju se tajnim bez obzira jesu li napisani rukom, osobnim računarom, strojem, štampani, stenografirani, šifrirani, filmirani, fotokopirani, snimljeni na magnetnoj traci, usb, hard diskovima, CD/DVD-u ili drugim medijima.

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

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

Član 8.

Tajne podatke su dužni čuvati izabrani dužnosnici, nositelji izvršnih funkcija i zaposlenici Grada Tuzla, koji imaju pristup podacima iz člana 7. ovoga Pravilnika.

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

Član 9.

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

III. ORGANIZACIJA ZAŠTITE SIGURNOSTI

1. Područje obuhvata zaštite

Član 10.

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

- zgrade,
- prostorije,
- mrežna infrastruktura,
- serveri,
- radne stanice,
- operativni sistemi,

- aplikacije,
- podaci i baze podataka i
- neumreženi i drugi sistemi IS-a Grada Tuzla.

Član 11.

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

2. Načini korištenja IS-a

Član 12.

Lični računari, samostojeći ili povezani u lokalne mreže, s pripadajućim programima i podacima, kao i ostala informatička oprema u vlasništvu Grada Tuzla smiju se koristiti isključivo za potrebe posla i u okviru ovlaštenja za obavljanje poslova.

Zabranjeno je koristiti lične računare i ostalu informatičku opremu, aplikacije i podatke izvan Grada Tuzla bez odobrenja ovlaštene osobe.

Član 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.

Član 14.

Tehničke zahvate na informatičkoj opremi (promjena konfiguracije, zamjena pojedinih dijelova opreme) smiju obavljati samo za to ovlaštene osobe koji su zaduženi za informatičku djelatnost ili ovlašteni serviseri uz nadzor administratora sistema uz pisani nalog.

Korisnicima informatičke opreme je zabranjeno obavljati tehničke zahvate iz prethodnog stava ovoga člana.

Član 15.

Korisnik smije koristiti samo odgovarajući potrošni materijal (optičke medije,papir,tinte za pisače i slično) kako ne bi nastale štete na informatičkoj opremi. Prilikom javne nabavke informatičke opreme i potrošnog materijala obavezno konsultovati administratora IS-a.

3. Ažurna evidencija svih računarskih i mrežnih resursa

Član 16.

Administratori sistema zaduženi su za vođenje ažurne evidencije o računarskim i mrežnim resursima IS-a Grada Tuzla.

Svako premještanje računara ili njihovih perifernih uređaja s jedne lokacije na drugu izvodi i evidentira ovlaštena osoba Stručne službe za poslove gradonačelnika i koordinaciju rada gradskih službi (u daljem tekstu: nadležna služba za poslove informatike).

Zastarjela oprema može se zamijeniti ili staviti van upotrebe samo od strane ovlaštene osobe nadležne službe za poslove informatike.

Član 17.

Premještanje računara i zamjenu zastarjele opreme izvodi ovlaštena osoba nadležne službe za poslove informatike.

4. Korisnici IS-a

Član 18.

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

Nadležna služba za poslove informatike dužna je voditi evidenciju o korisnicima IS-a Grada Tuzla.

Član 19.

Korisnicima IS-a Grada Tuzla iz člana 18. ovoga Pravilnika nadležna služba za poslove informatike dodjeljuje ovlaštenja za korištenje IS-a primjereno prirodi posla kojeg obavljaju, a po nalogu rukovodioca službe ili neposredno nadređenog službenika.

Korisnici ne smiju mijenjati instaliranu konfiguraciju bilo kojeg sistema informacija što obuhvata njihove radne stanice i prijenosne računare na način koji nije izričito dozvoljen od strane nadležne službe za poslove informatike.

Korisnici ne smiju mijenjati povezanost na mrežu svojih radnih stanica. Upotreba modema ili drugih uređaja za povezivanje radnih stanica sa vanjskim mrežama, što obuhvata i Internet zahtijeva ovlaštenje od strane nadležne službe za poslove informatike.

Korisnik IS-a je odgovoran ako instaliranje ili korištenje bilo kojeg nedozvoljenog softvera prouzrokuje da se sistem zaključa, padne ili da se djelomično ili potpuno izgube podaci.

Korisnici su odgovorni za zaštitu i back-up podataka na svom računaru. Ukoliko je korisniku potrebna stručna pomoć prilikom backup-a podataka može konsultovati administratore IS-a.

Korisnici ne smiju raditi bilo kakve kopije podataka o poslovanju, a koji se mogu naći pohranjeni na bilo kojem mediju, niti raditi kopije konfiguracijskih i sistemskih datoteka ili softvera u vlašnistvu Grada Tuzla.

5. Administratori IS-a

Član 20.

Administrator IS-a Grada Tuzla je autorizirani korisnik sa specijalnim ovlaštenjima za rad sa računarom, računarskim programima, bazama podataka, s ovlaštenjima pristupa do računara kao samostalne radne jedinice ili kao jedinice na mreži, a za potrebe administriranja i nadzora nad bazama podataka te administriranja, nadzora i upravljanja računarskom i mrežnom opremom.

Nadležna služba za poslove informatike dužna je voditi evidenciju o administratorima IS-a Grada Tuzla.

Član 21.

Administratoru IS-a Grada Tuzla iz člana 20. ovoga Pravilnika nadležna služba za poslove informatike dodjeljuje ovlaštenja za korištenje IS-a primjereno zahtjevima posla kojeg obavlja.

Član 22.

Instaliranje novih programa i izmjene postojećih programa smiju obavljati samo za to ovlaštene osobe nadležne službe ili ovlašteni serviseri uz nadzor administratora sistema uz pisani nalog.

Na servere ili lične računare smije se instalirati samo programska podrška za koju je dala saglasnost nadležna služba za poslove informatike .

Korištenje računarskog hardvera ili softvera koji nije nabavila Gradska uprava Tuzla, dozvoljeno je samo uz saglasnost nadležne službe za poslove informatike.

6. Održavanje sistema od strane vanjskih organizacija

Član 23.

Održavanje sistema od strane izabranih izvođača radova u postupku javnih nabavki provodi se uz saglasnost i po uputama zaposlenika nadležne službe za poslove informatike.

Svaka osoba koja po bilo kojoj osnovi obavlja u Gradu Tuzli privremene ili povremene poslove održavanja sistema, ili poslove temeljem posebnog ugovora, dužna je pridržavati se odredaba ovoga Pravilnika.

Član 24.

Nadležna služba za poslove informatike dužna je upoznati osobe navedene u članu 23. s odredbama ovoga Pravilnika pri davanju odobrenja za korištenje resursa IS-a Grada Tuzla.

7. Priključivanje i isključivanje servera i radnih stanica na mrežu

Član 25.

Korisnicima je zabranjeno priključivanje i isključivanje servera i radnih stanica na lokalnu mrežu bez ovlaštenja nadležne službe za poslove informatike.

8. Rad na daljinu (teleworking)

Član 26.

Bez prethodnog odobrenja nadležne službe za poslove informatike korisnicima je zabranjeno:

- povezivanje ličnih računara na Internet ili na neku drugu mrežu ili komunikacijski priključak izvan IS-a Grada Tuzla,

- spajanje računara izvan IS-a Grada Tuzla na računare i računarske sisteme Grada Tuzla.

Član 27.

O svim uočenim nepravilnostima u radu i korištenju informatičke opreme zaposleni Grada Tuzla je dužan odmah izvijestiti nadležnu službu za poslove informatike ili osobu odgovornu za provođenje mjera zaštite sigurnosti i provođenje sigurnosne politike.

IV. MJERE I SREDSTVA ZAŠTITE SIGURNOSTI

Član 28.

Prijetnje IS-u Grada Tuzla 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

Član 29.

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

Radi provođenja mjere dodjele pristupnih prava korisnicima mreže, aplikacija i baza podataka IS-a Grada Tuzla pohranjenih u računarima, nadležna služba za poslove informatike dužna je provoditi sljedeće radnje:

- organizovati i provjeravati autentičnost korisnika koji pristupaju mreži računarskih sistema,

- organizovati pristup i provesti kontrolu pristupa svim računarskim sistemima Grada Tuzla samo ovlaštenim djelatnicima primjereno zahtjevima posla kojeg obavljaju,

- omogućiti uređaje i softver za autentifikaciju za korisnike koji imaju velika ovlaštenja pristupa mreži i podacima,

- provesti sve nadopune, brisanja i promjene u organizaciji i kontroli pristupa računarskim sistemima u skladu s odobrenim zahtjevom krajnjeg korisnika,

- voditi i održavati ažurnim popis administrativnih pristupnih kodova i lozinki te čuvati taj popis na sigurnom mjestu,

- onemogućiti anonimni pristup bilo koje vrste do radnih stanica,

- kontrolisati modemske i slične priključke na mrežu

- odobriti instalaciju novih modema

Član 30.

Korisnik računarskog sistema je odgovoran za sve računarske transakcije izvršene uz upotrebu njegove korisničke identifikacije i lozinke.

Korisnik IS-a je dužan poštovati sljedeća pravila:

- zabranjeno je otkrivati lozinke drugima te se lozinka mora odmah 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 180 dana,

- ne smiju se koristiti lozinke koje se mogu lako pamtiti, lako odgonetnuti ili probiti od strane drugih,

- lozinke moraju sadržavati najmanje sedam znakova i to kombinaciju velikih i malih slova i brojki,

- korisnik mora odjaviti svoj account kada prestaje s radom na računaru duže od 1h,

- radna stanica se mora ugasiti kada nije u upotrebi (npr. preko noći).

Svi rukovodeći službenici gradskih službi Grada Tuzla su dužni odmah obavijestiti nadležnu službu za poslove informatike o tome da li nekom zaposlenom prestaje radni odnos u Gradu Tuzli ili se raspoređuje na rad u drugu službu, kako bi se mogla promjeniti njegova ovlaštenja za pristup resursima.

2. Zaštitni zid (FIREWALL)

Član 31.

Zaštitni zid (FIREWALL) 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:

- nadležna služba za poslove informatike je dužna:

- primijeniti zaštitni zid za organizaciju i kontrolu prometa podacima između vanjskog svijeta i unutrašnjeg dijela mreže,

- primijeniti zaštitni zid za sprječavanje nedozvoljenog prometa mrežom iznutra prema van,

- primijeniti zaštitni zid za sprječavanje nedozvoljenog prometa mrežom iz vanjskog svijeta prema unutrašnjem dijelu mreže,

- primijeniti zaštitni zid za sprečavanje nedozvoljenog prometa zaštićenim segmentom lokalne mreže od ostale lokalne mreže.

3. Internet i elektronska pošta

Član 32.

Sigurno korištenje Interneta i elektronske pošte provodi se u cilju sprečavanja zaraze računarskim 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.

Gradska uprava Grada Tuzla smatra Internet usluge kao sredstvo koje može značajno da poveća produktivnost. Zbog toga, korisnici imaju mogućnost da ga koriste zbog poslovnih interesa Gradske uprave Grada Tuzla.

Nadležna služba za poslove informatike obezbjeđuje opremu i parametre potrebne za pristup Internet uslugama. Strogo se zabranjuje modifikacija parametara na načine koji nisu odobreni od strane nadležne službe za poslove informatike

Usluge Interneta a posebno World Wide Weba (WWW) predstavljaju važne izvore informacija za Gradsku upravu Grada Tuzla. Iz razloga što ne postoji kontrola kvaliteta informacija koje su dostupne preko Interneta, informacije koje se preuzmu sa Interneta treba uvijek pažljivo koristiti.

Korisnicima nije dozvoljeno da preuzimaju softver sa Interneta u privatne svrhe.

Korisnicima nije dozvoljen pristup Internetu sa sistema računara koji sadrži stratešku informaciju čak i kada je nadležna služba za poslove informatike poduzela sve moguće mjere zaštite.

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

- dozvoljen je svaki oblik komunikacije putem Interneta (Društvene mreže,Forumi, Skype, Viber i sl.) koja se obavlja iz profesionalnih razloga i koja ne utječe negativno na produktivnost,

- dozvoljeno je korištenje web explorera za prikupljanje poslovnih informacija s komercijalnih web adresa,

- dozvoljeno je korištenje Interneta za pristup bazama podataka radi pronalaženja poslovnih informacija,

- nadležna služba za poslove informatike obezbjeđuje alat potreban za rad e-mail usluga. Strogo je zabranjena modifikacija ovih alata i korištenje alata koje nije nabavila nadležna služba za poslove informatike,

- Poruke koje obrađuje e-mail sistem Gradske uprave Grada Tuzla predstavljaju vlasništvo Gradske uprave Grada Tuzla,

- Korisnicima nije dozvoljen pristup računima koji nisu njima dodijeljeni ili da koriste e- mail sistem pod identitetom drugih korisnika,

- dozvoljeno je korištenje elektronske pošte u svrhu ostvarivanja poslovnih kontakata,

- za poslovnu komunikaciju obavezno je korištenje zvanične e-mail adrese koju korisniku dodjeljuje administrator IS-a,

- korisnik Interneta i elektronske 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 zaposlenog koji je obavlja,

- zabranjeno je slanje i prosljeđivanje lančane elektronske pošte, tj. poruka koje uključuju procedure za prosljeđivanje poruka drugima,

- zabranjeno je slanje iste poruke na više od deset (10) prijemnih adresa ili na više od jedne dostavne (distribucijske) liste, osim u slučajevima kada to priroda komunikacije zahtijeva,

- kada se korisniku dodjeljuje e-mail adresa potrebno je slijediti slijedeća uputstva: - E-mail adresa treba da sadrži:*imeprvoslovoprezimena@tuzla.ba*

- s vremena na vrijeme korisnici treba da izbrišu iz sistema poruke i priloge koji nisu od važnosti za poslove Gradske uprave Grada Tuzla. E-mail poruke koje su relevantne za poslove Gradske uprave Grada Tuzla i koje se moraju duže vremena čuvati treba spasiti izvan e-mail sistema u fajling sistem ili bazu podataka koju podržava adekvatan back-up sistem,

- ako korisnik primi poruku koja se ne odnosi na njega treba da obavijesti administratore IS-a i poduzme mjere da zaštiti tajnost poruke,

- korisnici ne smiju odgovarati na nepoznate e-mail poruke. Korisnici treba da imaju na umu da porijeklo e-mail poruke može biti falsifikovano ili adresa pošiljaoca korištena bez dozvole stvarnog vlasnika,

- zabranjeno je obavljanje privatnih i osobnih poslova uz korištenje resursa IS-a Grada Tuzla,

- zabranjeno je slanje bilo kakvog sadržaja koji je ofanzivan, koji primatelju može stvoriti neprilike ili štetu, ili je obmanjujući,

- antivirusna zaštita mora biti obavezno aktivirana kod prijema elektronske pošte i pridruženih datoteka,

- zabranjeno je pokretanje izvršnih datoteka ako se ne zna o čemu se radi i da li je izvor pouzdan. Korisnik treba da je svjestan opasnosti od virusa u korištenju e-mail sistema. Korisnici naročito treba da imaju na umu da prilozi uz e-mail mogu da sadrže viruse iako izgleda da je poruku poslao pouzdan korisnik,

- Zbog ograničenja u infrastrukturi komunikacija, nadležna služba za poslove informatike može da uvede ograničenje na dužinu korisnikovih e-mail poruka (odlazećih i dolazećih) kao i veličinu prostora određenog za pohranjivanje poruka,

- Politika Gradske uprave Grada Tuzla je da obezbijedi tehnička sredstva za povećanje stepena tajnosti, integriteta i dostupnosti e-mail usluga. Međutim, korisnici treba da imaju na umu da se ne može garantovati sigurnost e-mail poruka pogotovu kada e-mail porukama rukuju e-mail sistemi koji nisu pod direktnom kontrolom Gradske uprave Grada Tuzla ,

- osim ako se ne koriste odgovarajuće kriptografske tehnike, korisnici treba da izbjegavaju korištenje e-mail sistema za slanje osjetljivih informacija kao što su brojevi kreditnih kartica, lični podaci i informacije koje su označene kao *Ograničene* ili *Povjerljive,*

- osim ako se ne koriste tehnike potvrde vjerodostojnosti i integriteta korisnici treba da znaju da e-mail sistem ne može garantovati da je primljene poruke poslao dotični pošiljalac te da nisu usput bile izmijenjene,

- korisnici ne treba da šalju poruke na način koji se protivi propisima o zaštiti ličnih podataka ili drugim propisima u pogledu tajnosti podataka.

U slučaju zloupotrebe korištenja interneta i elektronske pošte od strane korisnika IS-a Grada Tuzla, a na zahtjev rukovodioca nadležne službe, administrator IS-a može ograničiti ili onemogućiti upotrebu interneta i elektronske pošte.

4. Antivirusna zaštita

Član 33.

Antivirusna zaštita provodi se u cilju sprečavanja zaraze računarskim 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 antivirusne zaštite potrebno je provoditi sljedeće radnje:

- nadležna služba za poslove informatike je dužna instalirati i održavati antivirusne programe na svim poslužiteljima i radnim stanicama Grada Tuzla redovnim ažuriranjem u pogledu novih vrsta virusa,

- nadležna služba za poslove informatike je dužna konfigurisati antivirusni program tako da vrši antivirusno skeniranje svih ulaznih objekata,

- nadležna služba za poslove informatike je dužna odgovoriti na sve napade računarskih virusa, uništiti svaki otkriveni virus te dokumentirati svaki incident,

- zabranjeno je namjerno unositi računarske viruse u računare Grada Tuzla,

- svako ko sumnja da je njegov računar zaražen virusom mora odmah isključiti računar i o tome obavijestiti administratora IS-a-

5. Korištenje softvera

Član 34.

Sigurno korištenje softvera provodi se u cilju sprečavanja zaraze računarskim 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,

- nadležna služba za poslove informatike je dužna voditi evidenciju o svim licencama softvera u posjedu Grada Tuzla,

- nadležna služba za poslove informatike je dužna periodično, a najmanje jednom godišnje, izvršiti uvid u računare u posjedu Grada Tuzla kako bi verificirao da je instaliran samo softver za čije korištenje je Grad Tuzla ovlašten,

- samo licencirani softver i softver u vlasništvu Grada Tuzla smije se instalirati na računarima Grada Tuzla,

- zabranjena je instalacija bilo kakvog softvera za koji se nema dozvola nadležne službe za poslove informatike,

- zabranjena je izmjena bilo kakvog softvera za koju se nema dozvola nadležne službe za poslove informatike,

- zabranjena je deinstalacija bilo kojeg softvera instaliranog na računaru bez dozvole nadležne službe za poslove informatike .

6. Zaštita podataka

Član 35.

Zaštita podataka provodi se u cilju sprečavanja zaraze računarskim 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.

Optičke medije (CD-ovi, DVD-ovi) , Hard diskove , USB i druge medije za pohranu podataka treba pohranjivati na sigurno mjesto kada se ne koriste. Ako sadrže krajnje osjetljive i povjerljive podatke moraju se zaključati.

Optičke medije (CD-ovi, DVD-ovi) , Hard diskove , USB i druge medije za pohranu podataka treba čuvati od opasnosti iz okruženja kao što je vrućina, direktna sunčeva svjetlost i magnetna polja.

Treba izbjegavati opasnosti koje prijete hardveru iz okruženja kao što je hrana, dim, tečnost, visoka ili niska vlažnost kao i krajnja vrućina ili hladnoća.

Korisnici treba da pažljivo čuvaju vrijednu elektronsku opremu koja im je dodijeljena.

Član 36.

Kako bi se postigla efikasna zaštita podataka, server mora biti opremljen:

- sistemom za sigurno prijavljivanje za rad sa mogućnošću evidentiranja ostvarenih pristupa, kako bi se pristup serveru mogao kontrolisati i ograničiti;
- mehanizmom za sprječavanje neovlaštenog iznošenja i unošenja podataka upotrebom prenosivih informatičkih medija, komunikacionih priključaka i priključaka za ispis podataka;
- mehanizmom zaštite od računarskih virusa i drugih štetnih programa.

Baze podataka obavezno se trebaju skladištiti na prenosive medije i to najmanje jednom sedmično, mjesečno i godišnje za potrebe obnove baze podataka.

Sedmično skladištenje podataka informacionog sistema vrši se posljednjeg radnog dana u sedmici, nakon sprovođenja dnevnog skladištenja podataka, u onoliko sedmičnih primjeraka koliko u mjesecu ima posljednjih radnih dana u sedmici.

Mjesečno skladištenje podataka informacionog sistema obavlja se posljednjeg radnog dana u mjesecu, za svaki mjesec posebno.

Godišnje skladištenje podataka informacionog sistema vrši se posljednjeg radnog dana u godini. Svaki primjerak godišnje uskladištenih podataka čuva se za vrijeme određeno propisima kojima se uređuje arhivska djelatnost. Svaki primjerak prenosivog medija sa uskladištenim podacima mora biti označen brojem, vrstom (sedmično, mjesečno, godišnje), datumom skladištenja, kao i imenom lica koje je izvršilo skladištenje podataka.

Upotrebljivost sigurnosne kopije podataka provjerava se najmanje svakih šest mjeseci, uz provjeru postupka povraćaja baza podataka uskladištenih na mediju, tako da vraćeni podaci nakon izvršene provjere budu cjeloviti, povjerljivi i dostupni za korištenje.
Puna zaštita (backup) za sve serverske mašine radi se obavezno jednom godišnje software-om za full-backup serverskih mašina, a po potrebi i češće (ukoliko je bilo izmjena u operativnom sistemu, dodavanja novih patch-eva, file-system-a i slično).

Član 37.

Svaki medij mora imati oznaku na kojoj su navedeni podaci o sadržaju.
Za izvorne programe mora biti navedeno:

-tačan naziv aplikacije;
-datum;

Svaki uređaj na kojima se štite podaci mora imati oznaku sa slijedećim podacima:

-aplikacija, odnosno grupa poslova,
-datum zaštite

- Za ostale korisnike, koji posao obavljaju na personalnom računaru, propisuje se isti način zaštite podataka na optičkim ili magnetnim medijima. Korisnici su sami dužni napraviti i čuvati ovu zaštitu u slučaju da hardwerski strada disk i na taj način im propadnu podaci (razne vrste korisničkih izvještaja).
Po isteku roka čuvanja podataka na medijima potrebno je nepovratno izbrisati sadržaj medija.

Član 38.

Nadležna služba za poslove informatike dužna je obezbijediti pristup „CLOUD“ servisima za potrebe backup-a baza podataka IS-a i dokumenata od važnosti za poslovanje gradske uprave Grada Tuzla.

7. Fizička zaštita prostorija s opremom

Član 39.

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:

- serveri i aktivna mrežna oprema se moraju smjestiti u sigurnim i čvrstim zgradama koje nisu izložene poplavi,

- serveri i mrežna oprema se moraju štititi stalnim izvorom energije (UPS), a ostala računarska oprema štiti se od strujnih udara stabilizatorima napona,

- prostorije sa serverima se moraju štititi od visoke ili niske vlažnosti zraka te ekstremne topline ili hladnoće klimatizacijskim uređajima,

- prostorije s računarskom opremom moraju biti zaštićene od požara u skladu sa Pravilnikom 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 računarskom opremom, vrata moraju biti zaključavana, a prozori zatvarani,

- u slučaju krađe ili gubitka ključa od prostorije s računarskom opremom treba obavijestiti odgovornu osobu i zamijeniti bravu,

- na sva vanjska vrata i prozore moraju biti instalirani uređaji za dojavu nasilnog ulaza i moraju se redovito kontrolisati,

- 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. PROVOĐENJE MJERA I SREDSTAVA ZAŠTITE SIGURNOSTI

1. Načini provođenja

Član 40.

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

Član 41.

Nadležna služba za poslove informatike neposredno organizira i nadzire provođenje mjera i sredstava zaštite sigurnosti utvrđenih ovim Pravilnikom.

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

Član 42.

Odgovorna osoba za provođenje mjera i sredstava zaštite sigurnosti pri obavljanju kontrole i nadzora nad provođenjem mjera zaštite sigurnosti dužna je

izvijestiti neposrednog rukovodioca kod kojeg je nadzor obavljen o rezultatima kontrole i unijeti ih u redovne izvještaje.

Ako odgovorna osoba za provođenje mjera zaštite sigurnosti pristupa rješavanju složenijih problema s područja zaštite sigurnosti IS-a sarađivat će sa svim stručnim službama.

Član 43.

Odgovorna osoba za provođenje mjera zaštite sigurnosti obavlja sljedeće poslove:

- obavlja redovnu kontrolu provođenje mjera zaštite sigurnosti utvrđenih ovim Pravilnikom,

- sarađuje i koordinira rad na izradi uputa za zaštitu sigurnosti IS-a,

- vodi brigu o pravovremenom osposobljavanju zaposlenih za zaštitu sigurnosti IS-a te vodi brigu o tome,

- izvještava pojedine rukovodioce o utvrđenim nepravilnostima u pogledu sigurnosnih uvjeta i predlaže mjere za otklanjanje istih.

Član 44.

Prilikom obavljanja kontrole provođenja mjera zaštite sigurnosti IS-a Grada Tuzla propisanih ovim Pravilnikom, odgovorna osoba ima sljedeća ovlaštenja:

- narediti prekid obavljanja posla ili radnje kojom se neposredno ugrožava sigurnost IS-a te o tome obavjestiti neposrednog rukovodioca,

- izvijestiti rukovodioca nadležne službe o neprovođenju propisanih mjera zaštite sigurnosti.

2. Subjekti provođenja

Član 45.

Svaki zaposleni u službama Grada Tuzla dužan je poduzimati i provoditi propisane mjere i sredstva zaštite sigurnosti IS-a Grada Tuzla u skladu s ovim Pravilnikom.

Član 46.

Rukovodioci službi obavezni su:

- provoditi i nadzirati provođenje propisanih mjera zaštite sigurnosti,

- upoznati novog zaposlenog s opasnostima od ugrožavanja sigurnosti IS-a Grada Tuzla,

- poduzeti mjere da se nedostaci koji mogu utjecati na sigurnost IS-a, a utvrđeni su pregledom ili prijavljeni od strane odgovorne osobe za provođenje 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,

- provjeriti da li su poduzete potrebne mjere zaštite sigurnosti sistema nakon završetka rada, a prije odlaska iz radnih prostora,

- prekinuti rad na radnom mjestu, na sredstvu rada i u radnoj okolini ako se utvrdi da postoji izravna opasnost za ugrožavanje sigurnosti sistema ili se poslovi izvode suprotno pravilima zaštite.

Član 47.

Zaposlenik u službama Grada Tuzla dužan je:

- upoznati se s odredbama ovog Pravilnika prije stupanja na rad i samostalnog obavljanja poslova na radnom mjestu, kao i svladati osposobljavanje za provođenje 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 sistema odmah prijaviti neposrednom rukovodiocu ili osobi odgovornoj za provođenje mjera zaštite sigurnosti.

3. Edukacija korisnika i administratora

Član 48.

Odgovorna osoba za provođenje mjera i sredstava zaštite sigurnosti dužna je osigurati osposobljavanje zaposlenika Grada Tuzla za provođenje mjera i sredstava zaštite propisanih ovim Pravilnikom.

Obaveza iz stava 1 ovoga člana odnosi se i na djelatnike koji su zaposleni na određeno vrijeme.

4. Korisnički i administratorski priručnici

Član 49.

Odgovorna osoba za provođenje 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 Tuzla u skladu s odredbama ovoga Pravilnika.

5. Postupanje u incidentnim situacijama

Član 50.

U slučaju havarije ili incidentne situacije djelatnik Grada Tuzla je dužan odmah obavjestiti odgovornu osobu za provođenje mjera zaštite sigurnosti.

Pod havarijom u smislu ovoga Pravilnika smatra se:

- potpuni gubitak sistema,
- gubitak programa,
- gubitak podataka.

Pod incidentnim situacijama u smislu ovoga Pravilnika smatraju se:
- privremeni prestanak rada sistema,
- gubitak opreme,
- ograničavanje resursa u radu,
- smanjenje resursa,
- kvar opreme
- sve drugo što može ugroziti IS grada Tuzla

6. Nadzor

Član 51.

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

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

7. Stalni i povremeni nadzor

Član 52.

Nadležna služba za poslove informatike za provedbu mjera i sredstava zaštite sigurnosti dužna je provoditi stalni i povremeni nadzor provedbe mjera i sredstava zaštite propisanih ovim Pravilnikom.

VI. ODGOVORNOST ZBOG NEPRIDRŽAVANJA MJERA I SREDSTAVA ZAŠTITE SIGURNOSTI

Član 53.

Osoba odgovorna za provođenje mjera zaštite sigurnosti i provođenje sigurnosne politike u skladu s ovim Pravilnikom je rukovodilac nadležne službe za poslove informatike Grada Tuzla.

Odgovorna osoba za provođenje mjera zaštite sigurnosti redovno obavlja kontrolu provođenja mjera zaštite utvrđenih ovim Pravilnikom i odgovorna je za provođenje tih mjera.

Član 54.

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

Ako korisnik nepridržavanjem odredaba ovoga Pravilnika nanese štetu Gradu Tuzli, odgovara za pričinjenu štetu .

VII. ZAVRŠNE ODREDBE

Član 55.

Svaki korisnik IS-a Grada Tuzla dužan je potpisati Izjavu o prihvatanju sigurnosne politike IS-a Grada Tuzla (Prilog 1).

Član 56.

Gradonačelnik GradaTuzla donijet će u roku od jedne godine dana od dana stupanja na snagu ovoga Pravilnika skup pravila, i to:

- Plan oporavka u slučaju havarije,
- Plan zaštite i povrata podataka,
- Plan provođenja protuvirusne zaštite,
- Plan postupanja u incidentnim situacijama,
- Oblici saradnje administratora s korisnikom.

Član 57.

Ovaj Pravilnik se može mijenjati i dopunjavati u zavisnosti od vlastititih potreba i/ili zbog obaveza nametnutih propisima viših organa vlasti.

Prijedlog za promjene pravilnika zbog razloga navedenih u prethodnom stavu, podnosi rukovodilac gradske službe, a podnosi ga Gradonačelniku Grada Tuzla putem nadležne službe za poslove informatike.

Član 58.

Svako postupanje koje je suprotno odredbama ovog Pravilnika smatra se zloupotrebom i prekoračenjem službenih ovlaštenja i podliježe disciplinskoj odgovornosti.

Član 59.

Pravilnik stupa na snagu osmog dana od dana objavljivanja u „Službenom glasniku Grada Tuzla“.

Bosna i Hercegovina
Federacija Bosne i Hercegovine
Tuzlanski kanton
GRAD TUZLA
GRADONAČELNIK
Broj: 02-_____
Tuzla, _____. godine

GRADONAČELNIK:

Jasmin Imamović, dipl. pravnik

Prilog 1.

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

Potpisivanjem ove Izjave izjavljujem da sam:

1. Primio i pročitao Pravilnik o sigurnosti Integralnog informacionog sistema Grada Tuzla i razumio ga.

2. Razumio sam i slažem se da svaki računar, softver i memorijski medij koji mi je nabavio Grad Tuzla sadrži vlasništvom zaštićene i povjerljive informacije o Gradu Tuzli i njenim poslovnim partnerima te da one jesu i ostaju vlasništvo Grada Tuzla u svim svojim dijelovima i trajno.

3. Slažem se da neću kopirati, umnožavati (s izuzetkom sigurnosnog kopiranja kao dijela mojih radnih obaveza u Gradu Tuzli), 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 Tuzli iz bilo kojeg razloga, odmah vratiti izvorni primjerak i sve kopije svog softvera, računarskog materijala i računarske opreme koje sam primio od Grada Tuzla, a koji su u mome posjedu ili na bilo koji drugi način pod mojom kontrolom.

_____

Ime i prezime zaposlenika:

_____

Služba:

_____

Datum:

_____

Potpis zaposlenika:

_____