



210315|0240325011|13

**REPUBLIKA HRVATSKA
BJELOVARSKO-BILOGORSKA
ŽUPANIJA
OPĆINA ŠANDROVAC
OPĆINSKI NAČELNIK**

**KLASA: 024-03/25-01/1
URBROJ: 2103-15-03-25-13
Šandrovac, 15 siječnja 2025. godine**

Na temelju članka 58. Statuta Općine Šandrovac („Općinski glasnik Općine Šandrovac“ broj 02/09, 18/11) u skladu s Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) i Zakonom o provedbi Opće uredbе o zaštiti podataka („Narodne novine“ broj 42/18.), općinski načelnik Općine Šandrovac dana 15.01.2025. godine donosi

**PRAVILNIK
o sigurnosti informacijskog sustava
Općine Šandrovac**

I. OPĆE ODREDBE

Članak 1.

Ovim se Pravilnikom utvrđuju:

- ciljevi zaštite sigurnosti Informacijskog sustava Općine Šandrovac (u daljnjem tekstu: IS)
- 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. 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 primarnoj 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 sustav autorizacije dozvolio pristup.
4. Lozinka (password) - jedinstveni red znakova koje zna samo korisnik.
5. Account - mrežno ime ili identitet korisnika koji radi na računalu priključenom na mrežu računala.
6. 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.
7. 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.
8. 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.
9. Kriptografija - matematički algoritmi i procesi kojima se dobivaju nečitljive poruke, kao i konverzija tih poruka u čitljivi tekst.
10. Enkripcija podataka - postupak pretvaranja čitljivih podataka u nečitljive (cypher text).
11. Dekriptiranje podataka - proces kod kojega se kodirani tekst vraća u prvobitno originalno stanje.
12. Vatrozid (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.
13. Elektronička pošta (e-mail) - 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: kolor fotografije, filmovi, animacije, dokumenti itd.
14. 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.
15. 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.
16. 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.
17. 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.
18. 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.

19. Softver - softver ili programska podrška za rad računala je niz instrukcija i podataka pohranjenih u elektroničkom obliku u računalu.

20. Operacijski sustav - operacijski sustav je skup osnovnih programa i alata koji pokreću računalu, upravljaju svim procesima u računalu, fizičkim i programskim dijelovima računala te uređuju njihovu komunikaciju.

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

22. 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.

23. Radna stanica - računalu 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.

24. Poslužitelji - poslužitelji su računala ili programski paketi koji omogućavaju specifičnu vrstu usluge za klijent programe koji se vrte na drugim računalima.

25. Klijent - klijent je računalu koje otvara i koristi programe i aplikacije sa servera ili preuzima s njega programe i podatke.

II. CILJEVI ZAŠTITE SIGURNOSTI IS-a

Članak 3.

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

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

Članak 4.

IS Općine 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 sredstva zaštite sigurnosti te utvrđivanja odgovornosti zbog nepridržavanja mjera i sredstva zaštite sigurnosti.

Članak 5.

IS Općine, u smislu ovoga Pravilnika, obuhvaća informacijske sustave Općine postavljene na središnjem mrežnom poslužitelju.

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

Članak 6.

Dostupnost podacima IS-a Općine 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 Općine.

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 Općine 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 Općine.

Članak 8.

Tajne podatke su dužni čuvati svi dužnosnici i djelatnici Općine, 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 Općine će postupiti u skladu sa Zakonom.

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 Općine.

Članak 11.

Mjere i sredstva zaštite sigurnosti IS-a Općine 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 Općine 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 službenog servisa sa kojim Općina ima sklopljen Ugovor (dalje: službeni servis), 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 (diskete, papir, trake, tinte za pisače i slično) i poštivati propisane procedure kod nabave i zamjene kako ne bi nastale štete na informatičkoj opremi.

3. Ažurna evidencija svih računalnih i mrežnih resursa

Članak 16.

Općina je nadležna za vođenje ažurne evidencije o računalnim i mrežnim resursima IS-a Općine.

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

Zastarjela oprema može se zamijeniti ili staviti izvan upotrebe samo od strane ovlaštene osobe službenog servisa.

Članak 17.

Premještanje računala i opreme izvodi ovlaštena osoba službenog servisa.

4. Korisnici IS-a

Članak 18.

Korisnik IS-a Općine 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.

Evidenciju o korisnicima IS-a Općine vodi službeni servis i Općina.

Članak 19.

Korisnicima IS-a Općine iz članka 18. ovoga Pravilnika Zavod za informatičku djelatnost dodjeljuje ovlasti za korištenje IS-a primjereno zahtjevima posla kojeg obavljaju.

5. Administratori IS-a

Članak 20.

Administrator IS-a Općine 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. Službeni servis i Općina su dužni voditi evidenciju o administratorima IS-a Općine.

Članak 21.

Administratoru IS-a Općine iz članka 20. ovoga Pravilnika službeni servis 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 Općine na prijedlog službenog servisa.

Službeni servis, u suradnji sa Općinom 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 službenog servisa uz nadzor djelatnika Općine, uz pisani nalog.

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

7. Održavanje sustava od strane vanjskih organizacija

Članak 24.

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

Svaka osoba koja po bilo kojoj osnovi obavlja u Općini 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 Općinu za vrijeme obavljanja tih poslova, dužni su provoditi mjere zaštite sigurnosti utvrđene ovim Pravilnikom.

Članak 25.

Službeni servis dužan je upoznati osobe navedene u članku 24. s odredbama ovoga Pravilnika pri davanju odobrenja za korištenje resursa IS-a Općine.

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 službenog servisa.

9. Rad na daljinu (teleworking)

Članak 27.

Bez prethodnog odobrenja Općine i službenog servisa, korisnicima je zabranjeno:

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

Članak 28.

O svim uočenim nepravilnostima u radu i korištenju informatičke opreme djelatnik Općine je dužan odmah izvijestiti službeni servis i načelnika Općine.

IV. MJERE I SREDSTVA ZAŠTITE SIGURNOSTI

Članak 29.

Prijetnje IS-u Općine 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 Općine.

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

- službeni servis je dužan organizirati i provjeravati autentičnost korisnika koji pristupaju mreži računalnih sustava,
- službeni servis je dužan organizirati pristup i provesti kontrolu pristupa svim računalnim sustavima Općine samo ovlaštenim djelatnicima primjereno zahtjevima posla kojeg obavljaju,
- službeni servis je dužan omogućiti uređaje i softver za autentifikaciju za korisnike koji imaju velika ovlaštenja pristupa mreži i podacima,
- službeni servis je dužan provesti sve nadopune, brisanja i promjene u organizaciji i kontroli pristupa računalnim sustavima u skladu s odobrenim zahtjevom krajnjeg korisnika,
- službeni servis je dužan voditi i održavati ažurnim popis administrativnih pristupnih kodova i lozinki te čuvati taj popis na sigurnom mjestu,
- službeni servis je dužan onemogućiti anonimni pristup bilo koje vrste do radnih stanica,
- službeni servis je dužan kontrolirati modemske i slične priključke na mrežu a instalaciju novih modema,

- službeni servis 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 pamtit, lako odgonetnuti ili probiti od strane drugih,
- lozinke moraju sadržavati najmanje sedam znakova i to kombinaciju slova, brojki i simbola,
- korisnik mora odjaviti svoj account kada prestaje s radom na računalu na duže vrijeme,
- kadrovska služba Općine je dužna promptno obavijestiti službenog serviseru o tome da li nekom djelatniku prestaje radni odnos u Općini ili se raspoređuje na rad u drug radno mjesto, 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:

- službeni servis je dužan primijeniti vatrozid za organizaciju i kontrolu prometa podacima između vanjskog svijeta i unutrašnjeg dijela mreže,
- službeni servis je dužan primijeniti vatrozid za sprječavanje nedozvoljenog prometa mrežom iznutra prema van,
- službeni servis je dužan primijeniti vatrozid za sprječavanje nedozvoljenog prometa mrežom iz vanjskog svijeta prema unutrašnjem dijelu mreže,
- službeni servis 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:

- službeni servis je dužan omogućiti korisnicima korištenje programa za kriptiranje podataka na disku i kriptiranje/dekriptiranje elektroničke pošte,
- službeni servis je dužan primijeniti virtualnu privatnu kriptiranu vezu (VPN) za prijenos podataka za korisnike vezane base-band i dial-up modemima na mrežu,
- službeni servis je dužan omogućiti korisnicima korištenje računalne opreme ili programa za izradu i verificiranje elektroničkog potpisa za identifikaciju potpisnika i vjerodostojnost potpisanog elektroničkog dokumenta,

- službeni servis 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) prijarnih adresa ili na više od jedne dostavne (distribucijske) liste,
- zabranjeno je obavljanje privatnih i osobnih poslova uz korištenje resursa IS-a Općine,
- 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 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:

- instalirati i održavati antivirusne programe na svim poslužiteljima i radnim stanicama Općine redovitim ažuriranjem u pogledu novih vrsta virusa,
- konfigurirati antivirusni program tako da vrši antivirusno skeniranje svih ulaznih objekata,
- odgovoriti na sve napade računalnih virusa, uništiti svaki otkriveni virus te dokumentirati svaki incident,
- zabranjeno je namjerno unositi računalne viruse u računala Općine,
- 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,
- Općina je dužna voditi evidenciju o svim licencama softvera u posjedu Općine,
- službeni servis je dužan periodično, a najmanje jednom godišnje, izvršiti uvid u računala u posjedu Općine kako bi verificirao da je instaliran samo softver za čije korištenje je Općina ovlaštena,
- samo licencirani softver i softver u vlasništvu Općine smije se instalirati na računalima Općine,
- zabranjena je instalacija ili izmjena bilo kakvog softvera za koju se nema suglasnost službenog servisa,
- zabranjena je deinstalacija bilo kojeg softvera instaliranog na računalu bez dozvole službenog servisa.

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,
- svi poslovni podaci po instaliranju diskovnog podsistema pohranjuju se na diskovni podsistem i osiguravaju se od strane službenog servisa.

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 zgradama 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,
- 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,
- oprema koja mora biti smještena na javno pristupnom prostoru mora biti zaštićena, a javni pristup nadziran,
- nepoznate osobe moraju pružiti dokaze o svojem identitetu,
- 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 Općine provodi se u skladu s odredbama ovoga Pravilnika.

Članak 39.

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.

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 pojedine pročelnike odjela gradske uprave o utvrđenim nepravilnostima glede sigurnosnih uvjeta i predlaže mjere za otklanjanje istih.

Članak 42.

Prigodom obavljanja kontrole provedbe mjera zaštite sigurnosti IS-a 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 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 Općini dužan je poduzimati i provoditi propisane mjere i sredstva zaštite sigurnosti IS-a Općine u skladu s ovim Pravilnikom.

Članak 44.

Načelnik Općine obvezan je:

- provoditi i nadzirati provođenje propisanih mjera zaštite sigurnosti,
- upoznati novog djelatnika s opasnostima od ugrožavanja sigurnosti IS-a Općine,
- 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 Općini 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 Općine 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.

4. Korisnički i administratorski priručnici

Članak 47.

Odgovorna osoba za provedbu mjera i sredstava zaštite sigurnosti po potrebi će osigurati korisničke i administratorske priručnike.

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

5. Postupanje u incidentnim situacijama

Članak 48.

U slučaju havarije ili incidentne situacije djelatnik Općine 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 Općine 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 načelnik Općine.

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 Općine je dužan pridržavati se svih mjera i sredstava zaštite propisanih ovim Pravilnikom.

Ako korisnik nepridržavanjem odredaba ovoga Pravilnika nanese štetu Općini, odgovara za pričinjenu štetu sukladno Zakonu i općem aktu Općine.

VII. ZAVRŠNE ODREDBE

Članak 53.

Svaki korisnik IS-a Općine dužan je potpisati Izjavu o prihvaćanju sigurnosne politike IS-a Općine.

Obrazac Izjave iz stavka 1. ovoga članka nalazi se u prilogu (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 Općine.

Članak 55.

Danom stupanja na snagu ovog Pravilnika stavlja se izvan snage Pravilnik o sigurnosti informacijskog sustava Općine Šandrovac (KLASA: 011-01/13-03/10, URBROJ: 2123-05-03-13-1 od 21.06.2013. godine.

Članak 55.

Ovaj Pravilnik stupa na snagu danom donošenja a objaviti će se na mrežnim stranicama općine Šandrovac.

Općinski načelnik Općine Šandrovac:

Dario Halauš, mag.ing.agr.



Prilog 1

**REPUBLIKA HRVATSKA
BJELOVARSKO-BILOGORSKA
ŽUPANIJA
OPĆINA ŠANDROVAC
OPĆINSKI NAČELNIK**

**I Z J A V A
O PRIHVAĆANJU SIGURNOSNE POLITIKE
INFORMACIJSKOG SUSTAVA OPĆINE ŠANDROVAC**

Potpisivanjem ove Izjave izjavljujem da sam:

1. Primio i pročitao Pravilnik o sigurnosti Integralnog informacijskog sustava Općine Šandrovac i razumio ga.
2. Razumio sam i slažem se da svako računalo, softver i memorijski medij koji mi je pribavila Općina Šandrovac sadrži vlasništvom zaštićene i povjerljive informacije o Općini Šandrovac i njenim poslovnim partnerima te da one jesu i ostaju vlasništvo Općine Šandrovac u svim svojim dijelovima i trajno.
3. Slažem se da neću kopirati, umnožavati (s izuzetkom sigurnosnog kopiranja kao dijela mojih radnih obveza u Općini Šandrovac), 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 Općini Šandrovac iz bilo kojeg razloga, odmah vratiti izvorni primjerak i sve kopije svog softvera, računalnog materijala i računalne opreme koje sam primio od Općine Šandrovac a koji su u mome posjedu ili na bilo koji drugi način pod mojom izravnom ili neizravnom kontrolom.

Potpis zaposlenika:

Ime i prezime zaposlenika:

Datum: _____