Na podlagi 38. člena Zakona o tajnih podatkih (Uradni list RS, št. 50/06-UPB2) in 6. člena Zakona o dostopu do informacij javnega značaja (ZDIJZ-UPB2, Uradni list RS, št. 51/2006) v povezavi z 39. in 40. členom Zakona o gospodarskih družbah (ZGD-1-UPB3-Uradni list RS, št. 65/2009) župan Občine Šentjernej izdaja naslednji

PRAVILNIK
O DOLOČITVI, RAVNANJU IN VAROVANJU ZAUPNIH PODATKOV

I.
Splošne določbe

1. člen

S tem pravilnikom je opredeljen enoten sistem določanja, ravnanja, varovanja in dostopa do zaupnih podatkov z delovnega področja Občine Šentjernej (v nadaljevanju: občina). Pravilnik določa nadzor in odgovornost nad izvajanjem določil ter ukrepe v primeru kršitve določil tega pravilnika.

Po tem pravilniku morajo ravnati funkcionarji občine, javni uslužbenci občine in zunanji sodelavci, ki opravljajo delo v občini (v nadaljevanju: uslužbenci).

2. člen

Posamezni izrazi v Pravilniku imajo naslednji pomen:

1. Zaupen podatek je dejstvo ali sredstvo z delovnega področja občine, ki se nanaša na tajen podatek ali poslovno skrivnost, katere razkritje bi za občino predstavljalo škodljive posledice;
2. Tajen podatek je dejstvo ali sredstvo, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga po Zakonu o tajnih podatkih določi in označi pooblaščena oseba in ki ga je treba zavarovati pred nepoklicanimi osebami;
3. Poslovna skrivnost so tisti materializirani (zapisi, načrti, sheme, diagrami, ipd.) in nematerializirani (vsako ustno seznanjanje s podatki, idejami, razgovorih, ipd.) podatki, informacije in stvaritve (v nadaljevanju: podatki), ki so z zakonom, tem pravilnikom, drugim aktom občine ali sklepom uprave oziroma odločitvijo pooblaščene osebe razglašeni za poslovno skrivnost in so tako pomembni, da so z njihovo izdajo očitno nastale ali bi lahko nastale take posledice, ki bi škodljivo vplivale na uspešno delo občine;
4. Dokument, listina ali gradivo (v nadaljevanju: dokument) je vse pisano (ročno, s pisalnim strojem, osebnim računalnikom, magnetni zapisi, digitalni posnetki), tiskano, risano, fotokopirano, posneto - filmano in drugo za trajno ali začasno shranjevanje podatkov;
5. Dokument, ki je zaupen, je vsak dokument, ki je napisan, narisan, natisnjen, razmnožen, posnet, fotografiran, magneten, optičen ali kakšen drugačen zapis tajnega podatka ali poslovne skrivnosti;

6. Dostop do podatkov, ki so za občino zaupni, je seznanitev osebe s tajnim podatkom ali možnost osebe pridobiti tajni podatek na podlagi dovoljenja za dostop do tajnih podatkov ali s poslovno skrivnostjo na podlagi trajnega pooblastila ali dovoljenja pooblaščene osebe;
7. Omejen dostop do podatkov, ki so za občino zaupni, je seznanitev osebe le z določeno vrsto zaupnosti na podlagi trajnega pooblastila ali enkratnega dovoljenja pooblaščene osebe;
8. Določanje zaupnosti je dejanje ali postopek, s katerim se podatek v skladu z zakonom ali s tem pravilnikom oceni za tajen podatek ali poslovno skrivnost in se mu določi stopnja in rok zaupnosti;
9. Varovanje zaupnih podatkov pomeni izvajanje ukrepov in postopkov, s katerimi se nepooblaščeni osebi prepreči seznanitev s tajnimi podatki ali poslovno skrivnostjo;
10. Nosilci zaupnih podatkov so papirnati dokumenti, diskete, CD, USB, filmski ali magnetni trakovi ali druga tehnična sredstva, ki omogočajo zapis podatka, ki je zaupen;
11. Prenos ali pošiljanje podatka, ki je zaupen, je vsako fizično ali tehnično dejanje z namenom, da se s tajnim podatkom ali poslovno skrivnostjo seznanijo osebe, ki imajo dostop do teh podatkov;
12. Medij je vsako sredstvo za shrambo, prenos in/ali pošiljanje tajnih podatkov ali poslovne skrivnosti;
13. Pooblaščena oseba je oseba, ki se jo s posebnim dovoljenjem ali sklepom pooblasti za izvajanje zakonskih določil in določil tega pravilnika in je v tej zvezi odgovorna županu;
14. Nepooblaščena oseba je vsaka oseba, ki nima dostopa do zaupnih podatkov;
15. Tretja oseba je vsaka oseba, ki ni zaposlena v družbi, niti ne deluje v organih družbe;
16. Prenehanje zaupnosti podatka je zakonita sprememba tajnega podatka ali poslovne skrivnosti v podatek, ki je dostopen v skladu s splošnimi predpisi, ki urejajo poslovanje občine;
17. Varnostno preverjanje osebe je poizvedba, ki jo pred izdajo dovoljenja za dostop do tajnih podatkov opravi pristojni organ in katere namen je zbrati podatke o morebitnih varnostnih zadržkih;
18. Varnostni zadržki so ugotovitve varnostnega preverjanja, iz katerih izhaja, da obstajajo dvomi o zanesljivosti in lojalnosti osebe, ki naj bi dobila dovoljenje za dostop do tajnih podatkov;
19. Obravnavanje zaupni podatkov (tajnih podatkov in poslovne skrivnosti) je določanje, označevanje, dostop, uporaba, evidentiranje, razmnoževanje, posredovanje, prenos, uničevanje nosilcev zaupnih podatkov, hramba, arhiviranje ter drugi ukrepi in postopki, s katerimi se zagotavlja njihova varnost.

II.
Določitev zaupnih podatkov

3. člen

Zaupen podatek lahko določi le oseba, ki je določena z zakonom ali s tem pravilnikom.

4. člen

Za zaupen podatek se ne more določiti podatek, ki je po svojem značaju javen ali podatek, ki bi pomenil kršitev zakona ali interesa javnega značaja.

5. člen

Za zaupne podatke štejejo tudi:

- občutljivi osebni podatki zaposlenih, poslovnih ali interesnih partnerjev in pogodbenih strank ter drugih oseb, za katere družba zbira podatke,
- podatki občine s področja varovanja in zaščite ter,
- drugi podatki določeni s sklepom občine.

6. člen

V dvomu je šteti, da je podatek zaupen.

7. člen

Le tisti, ki je določil zaupnost podatka, jo lahko tudi prekliče.

Določitev tajnih podatkov:

8. člen

Tajni podatek se določi za tajnega ob pogojih in na način določenih v Zakonu o tajnih podatkih.

Določitev poslovne skrivnosti:

9. člen

Za poslovno skrivnost se poleg podatkov določenih z zakoni štejejo tudi podatki, ki se nanašajo na:

- strateške odločitve poslovanja občine,
- finančne in denarne tokove ter likvidnost in solventnost občine,
- poslovne pogodbe in vsebine poslovnih razgovorov do sklenitve poslovne pogodbe,
- aktivnosti, ki se vodijo po Zakonu o javnem naročanju,
- ponudbe za naročila ali licitacije, dokler ni uradno objavljen izid naročanja,
- načrtovanje in izvajanje razvojnih, raziskovalnih, projektnih, analitskih aktivnosti in njihove rezultate,
- gesla in kode za vstop v računalniške programe ter šifriranje,
- podatki v zvezi s poslovanjem in zaposlenostjo pogodbenih strank,
- drugi podatki, ki jih kot poslovno skrivnost določi župan, občinska uprava ali pooblaščena oseba.

10. člen

Direktor občinske uprave (v nadaljevanju: direktor) določi dokument kot poslovno skrivnost in rok trajanja ob njegovem nastanku oziroma ob začetku izvajanja naloge, katere rezultat bo vseboval podatek, ki je poslovna skrivnost.

Kadar samo manjši del dokumenta vsebuje podatke, ki so poslovna skrivnost, je potrebno takšen del dokumenta izločiti in ga kot posebno prilogo priložiti dokumentu z oznako »poslovna skrivnost«.

11. člen

Vsak uslužbenec je dolžan v okviru svojih delovnih nalog oziroma pristojnosti presojati poslovni ali varnostni pomen podatkov in predlagati direktorju določitev teh podatkov za poslovno skrivnost, če meni, da je to potrebno.

12. člen

Pripravljavci dokumentov s podatki, ki so poslovna skrivnost, že v fazi priprave gradiva postopajo v skladu s tem pravilnikom in predlagajo direktorju določitev poslovne skrivnosti in rok trajnosti.

13. člen

Za dokumente, katerim je poslovno skrivnost določila tretja oseba, se ravna po določilih splošne zakonodaje in tega pravilnika.

III.
Označevanje dokumentov, ki so zaupni

14. člen

Vsak zaupen podatek oziroma vsak dokument, ki vsebuje zaupne podatke, mora biti označen z vrsto zaupnosti.

Označevanje tajnih podatkov oziroma dokumentov, ki vsebujejo tajne podatke:

15. člen

Označevanje tajnih podatkov oziroma dokumentov, ki vsebujejo tajne podatke, se izvaja ob pogojih in na način, določenih v Zakonu o tajnih podatkih.

Označevanje poslovne skrivnosti oziroma dokumentov, ki vsebujejo poslovno skrivnost:

16. člen

Dokumenti, ki so poslovna skrivnost, se označujejo in vodijo, kot to za take primere zahtevajo pravila pisarniškega poslovanja.

17. člen

Dokumenti, ki so poslovna skrivnost, morajo biti ob določitvi poslovne skrivnosti vidno in v neskrajšani obliki na desnem gornjem kotu naslovne strani dokumenta označeni z oznako »POSLOVNA SKRIVNOST«.

V kolikor ni možno označiti dokument na desnem gornjem kotu, se ga označi na drugem vidnem mestu dokumenta.

Pod napisom poslovna skrivnost se označi datum določitve poslovne skrivnosti in po potrebi datum prenehanja.

18. člen

Če gre za pomembnejši ali obsežnejši dokument se pod označbami, določenimi v prejšnjem členu, dodajo še podatki:

- številka izvoda
- oštevilčenje strani glede na skupno število strani dokumenta
- morebitne priloge in spremljajoči dokumenti
- število izdelanih kopij

19. člen

Označba »POSLOVNA SKRIVNOST« se mora jasno razlikovati od drugih zapisov, pri čemer se za zapis označbe uporabijo tiskane črke, ki morajo biti večje od črk preostalih zapisov.

20. člen

Vse kopije dokumenta morajo biti označene kot izvirni dokument. Pri številki izvoda se označi zaporedna številka kopije.

Kopija se lahko označi tudi tako, da se onemogoči nadaljnje razmnoževanje oziroma prepreči nekontrolirano razmnoževanje.

21. člen

Ko prenehajo razlogi za poslovno skrivnost, se oznake izbrišejo in navede, kdo in kdaj je določil prenehanje.

22. člen

Predlogi, osnutki ali delovna gradiva, ki vsebujejo podatke, ki so poslovna skrivnost, se označuje in z njimi postopa enako, kot z originalnimi dokumenti.

V primeru posredovanja delovnega gradiva se ga evidentira in obravnava po predpisih pisarniškega poslovanja in določilih tega pravilnika, tako, da se pod »POSLOVNA SKRIVNOST« pripiše »DELOVNO GRADIVO«.

IV.
Splošni varnostni ukrepi

23. člen

S podatki, ki so opredeljeni kot zaupni, so lahko seznanjeni samo tisti uslužbenci, ki so jim potrebni za opravljanje njihovih delovnih nalog in funkcij.

Vsak uslužbenec, ki mu je bil zaupan tajni podatek ali poslovna skrivnost, ali je bil seznanjen z njeno vsebino, je odgovoren za njegovo varovanje in ohranitev njene zaupnosti.

Uslužbenec, ki se je v okviru svojega dela seznanil z zaupnimi podatki, teh ne sme uporabiti za druge namene kot za izvajanje delovnih nalog ali funkcij v občini.

24. člen

Dolžnost varovanja nastane v trenutku, ko se uslužbenec ne glede na način seznani z zaupnim podatkom. Dolžnost varovanja časovno ni omejena in traja dokler obstajajo razlogi za varovanje zaupnosti, razen če direktor ne določi drugače.

Dolžnost varovanja traja dokler direktor ne določi, da je prenehala potreba po varovanju.

25. člen

Zaupne podatke se mora v občini hraniti na način, ki zagotavlja, da imajo dostop do teh podatkov samo uslužbenci, ki podatke potrebujejo za izvajanje svojih delovnih nalog ali funkcij.

26. člen

S postopki in ukrepi varovanja zaupnih podatkov se:
- zagotavlja molčečnost,
- varujejo dokumenti, objekti, prostori, mediji, tehnična in druga sredstva, programska in druga strojna oprema,
- zagotavlja varno obravnavanje in hramba podatka, ki je zaupen,
- zagotavlja varno posredovanje, prenos in pošiljanje podatka, ki je zaupen,
- omogoča naknadno ugotavljanje odgovornosti ob kršitvah določil tega pravilnika.

27. člen

Za neposredno izvajanje postopkov in ukrepov za varovanje zaupnih podatkov je odgovoren direktor občinske uprave, ki mora:

- poslovanje organizirati tako, da se zagotovi spoštovanje določb s področja zaupnih podatkov iz Zakona o tajnih podatkih, Zakona o gospodarskih družbah, zakonodaje, ki ureja delovanje lokalne samouprave, njihovih podzakonskih aktov ter določb tega pravilnika;
- seznaniti uslužbence z dolžnostjo varovati zaupne podatke.

28. člen

Uslužbenci so dolžni izvajati naslednje varnostne ukrepe:

- zaklepati pisalne mize, omare, blagajne in pisarne, v katerih hranijo zaupne podatke, ko niso na svojem delovnem mestu;
- poskrbeti, da v prisotnosti oseb, ki niso zaposlene v občini, na pisalnih mizah ni delovnih dokumentov oziroma da se nepooblaščenim osebam onemogoči vpogled v delovne dokumente;
- dosledno izvajati postopek prijave oziroma odjave s svojim osebnim geslom na začetku oziroma ob zaključku računalniškega obravnavanja podatkov oziroma z uporabo gesla preprečiti dostop nepooblaščenim osebam do dokumentov;
- po končani izdelavi dokumentov z zaupnimi podatki poskrbeti za uničenje delovnega gradiva nastalega pri izdelavi dokumentov;
- upoštevati druge predpise na področju obravnavanja in varovanja tajnih podatkov oziroma poslovne skrivnosti.

29. člen

Če uslužbenci ugotovijo, da je prišlo do izgube zaupni podatkov ali do nepooblaščenega razkritja zaupnih podatkov, morajo o tem nemudoma obvestiti direktorja.

Direktor mora takoj ukreniti vse potrebno, da se ugotovijo okoliščine, zaradi katerih je prišlo do izgube ali razkritja zaupnega podatka nepoklicani osebi, da se odpravijo škodljive posledice in prepreči ponovna izguba oziroma nepooblaščeno razkritje zaupnega podatka.

30. člen

Dostop do podatkov, ki so zaupni, je možen le na podlagi izdanega pooblastila ali dovoljenja, ki ga izda direktor.

Direktor lahko izda pooblastilo uslužbencu za celovit trajen oziroma omejen trajen ali omejen začasen dostop do zaupnih podatkov.

31. člen

Notranji nadzor nad izvajanjem tega pravilnika izvaja direktor ali v skladu z usmeritvami direktorja uslužbenec, katerega on pooblasti.

32. člen

Uslužbenec, ki krši dolžnosti varovanja zaupnih podatkov, je disciplinsko odgovoren za hujšo kršitev delovnih obveznosti in dolžnosti.

V.
Varovanje prostorov

33. člen

Zaupni podatki se lahko obdelujejo in hranijo le v prostorih občine, ki so z organizacijskimi ter fizičnimi in tehničnimi ukrepi varovani tako, da onemogočajo nepooblaščenim osebam dostop do njih.

Zaupni podatki se morajo hraniti na način, ki zagotavlja, da imajo dostop do njih le pooblaščeni uslužbenci, v ognjevzdržnih omarah oziroma blagajnah ustrezne protivlomne stopnje ali tako, da onemogočajo nepooblaščenim osebam dostop do njih.
Zaupni podatki in mediji, ki so hranjeni izven aktivnih delovnih prostorov oziroma izven tehnično varovanih prostorov, morajo biti stalno zaklenjeni v ognjevarni in protivlomno zaščiteni omari.

Ključe ali posamezno nastavitev kombinacije elektronskih ključavnic sme imeti le direktor ali uslužbenec, ki se ga pooblasti.

Rezervni ključi oziroma kombinacija se hrani v zapečateni kuverti na varnem mestu.

Za obravnavanje in hranjenje dokumentov, ki vsebujejo tajne podatke, stopnje tajnosti ZAUPNO, TAJNO in STROGO TAJNO, veljajo še določbe iz Uredbe o varovanju tajnih podatkov (Uradni list RS, št. 74/05).

34. člen

Delo in gibanje v prostorih občine poteka v skladu s hišnim redom oziroma drugimi navodili direktorja ter ob spoštovanju požarnovarnostnih ukrepov.

Za varovanje prostorov, kjer se hranijo dokumenti, ki vsebujejo tajne podatke, se izvajajo še dodatni varnostni ukrepi:
- obiski zunanjih strank so dovoljeni samo z odobritvijo direktorja in potekajo v spremstvu uslužbenca:
- velja prepoved uporabe odprtega ognja in hramba hitro gorljivih in eksplozivnih snovi;
- ognjevarne omare, v katerih so shranjeni mediji, morajo biti vedno zaklenjene.

VI.
Varovanje dokumentov in medijev, ki vsebujejo zaupne podatke

35. člen

Direktor določi uslužbenca za vodenje evidence dostopa do dokumentov, ki vsebujejo zaupne podatke.

Iz evidence vpogledov mora biti razvidno, kdo in kdaj je opravil vpogled oziroma komu in kdaj so bili zaupni podatki posredovani.

VII.
Varovanje komunikacij, po katerih se prenašajo zaupno podatki

36. člen

Komunikacije za prenos zaupnih podatkov, ki so v lasti občine, varuje uslužbenec, ki ga pooblasti direktor.

VIII.
Varovanje in zaščita zaupnih podatkov na elektronskih medijih

37. člen

Za zaščito in varovanje zaupnih podatkov na elektronskih medijih se izvajajo posebni ukrepi, ki minimizirajo možnost izgube podatkov in dostop do podatkov nepooblaščenim osebam.

Direktor določi zaupnim podatkom način zaščite elektronskih medijih.

Za izvajanje varovanja in zaščite zaupnih podatkov na elektronskih medijih so odgovorni vsi njeni uporabniki.

38. člen

Računalniki in strežniki notranje mreže se lahko nahajajo le v varovanih prostorih občine.

Strojno in programsko opremo uporabljajo le uslužbenci. Poleg njih imajo dostop do te opreme tudi pogodbeno vezani zunanji sodelavci, ki so seznanjeni z določbami tega pravilnika.

Strojno in programsko opremo je dovoljeno uporabljati le za izvajanje nalog občine.

39. člen

Dostop do strojne in programske mora biti varovan tako, da dovoljujejo dostop samo pooblaščenim uslužbencem. Vsak poseg se vpiše v administratorjevi evidenci.

Vsak poseg v strojno in programsko opremo je dovoljen samo z odobritvijo direktorja.

40. člen

Dostop do dokumentov ali aplikacij, ki vsebujejo zaupne podatke, se varujejo s sistemom identifikacije uporabnika.

Gesla za dostop do zaupnih podatkov se hranijo v zapečatenih ovojnicah na posebno zavarovanem mestu in se jih ne sme posojati.

Računalniki oziroma računalniško omrežje občine in vanj vklopljene naprave morajo biti pred nepooblaščenim dostopom varovane s požarnimi pregradami in protivirusno opremo.

41. člen

Splošni varovalni ukrepi za odgovorno osebo, ki skrbi za informacijski sistem, so:

- zaščita pred zunanjimi vdori v računalniško omrežje družbe,
- zaščita server računalnikov in omrežja,
- zaščita arhivskih in varnostnih kopij dokumentov, ki so poslovna skrivnost,
- zagotavljanje in izvajanje sistema pristopnih gesel za dostop do omrežja družbe in posameznih njenih aplikacij.

42. člen

Splošni varovalni ukrepi uporabnikov v omrežju so:

- dosledna uporaba osebnih gesel,
- preprečitev fizičnega dostopa do osebnih računalnikov nepooblaščenim osebam,
- sprotno odjavljanje iz aplikacij, ko ostane računalnik brez nadzora, oziroma z geslom zaščiten ohranjevalnik zaslona,
- preprečitev priklopa na omrežje družbe vsakega računalnika zunanjega izvora,
- v primerih, ko se dokument, ki je poslovna skrivnost, nahaja na osebnem računalniku, je uporabnik dolžan zagotoviti ustrezno varnost in zaščito podatkov z ukrepi kot so: strožja fizična zaščita, dodatna zaščita osebnega računalnika oziroma dokumentov, ki so poslovna skrivnost, z geslom, hranjenje varnostnih kopij na varovanem mestu, šifriranje.

IX.
Prenos in pošiljanje zaupnih podatkov

43. člen

Zaupni podatki se lahko prenašajo in pošiljajo izven prostorov občine izključno ob upoštevanju varnostnih ukrepov in postopkov, ki morajo zagotoviti, da jih prejme izključno naslovnik oziroma oseba, ki je do teh podatkov upravičena.

Po pošti se zaupne podatke pošilja priporočeno s povratnico.

Pri prenosu zaupnih podatkov po kurirju se le-te prenaša v zaprti ustrezno označeni ovojnici. Naslovnik ali oseba, ki jo naslovnik pooblasti, potrdi prejem zaupnih podatkov z vpisom v dostavno knjigo.

Po elektronski pošti in faksu se smejo pošiljati le ustrezno šifrirani zaupni podatki.

Za elektronsko pošiljanje zaupnih dokumentov znotraj omrežja (intranet) morajo biti datoteke zavarovane z geslom (lahko tudi z geslom samo za branje). Elektronski naslov mora vsebovati opozorilo, kako ravnati z zaupno informacijo in kako ravnati, če je bil pri prenosu dokument pomotoma poslan na drug naslov.

Za elektronsko pošiljanje zaupnih dokumentov izven omrežja občine (internet) se mora dokument pred pošiljanjem v omrežje šifrirati po standardih za šifriranje. Po potrebi morajo biti datoteke zavarovane z geslom za odpiranje samo za branje.

V primeru bojazni, da elektronsko pošiljanje ni varno, njegova uporaba ni dovoljena.

Zaupni podatki se ne smejo prenašati ali posredovati po nezaščitenih komunikacijskih sredstvih.

44. člen

Tajni podatki stopnje zaupnosti ZAUPNO, TAJNO in STROGO TAJNO se smejo prenašati le s kurirsko službo.

Za tajne podatke iz prvega odstavka tega člena občina vodi seznam vpogledov v pisni dokument, v katerem se vodijo naslednji podatki:

- kratka vsebina zadeve, datum, stopnja tajnosti, številka izvoda dokumenta, ki vsebuje tajni podatek;
- ime in priimek osebe, ki se je seznanila s tajnim podatkom;
- razlog seznanitve;
- datum in čas seznanitve;
- podpis osebe, ki se je seznanila s tajnim podatkom.

X.
Razmnoževanje zaupnih dokumentov

45. člen

Zaupni dokumenti se ne smejo razmnoževati, kopirati ali prepisovati, razen če tako ne odredi direktor.

Direktor odredi število kopij in komu se kopije posredujejo. Vsaka kopija zaupnega dokumenta se ustrezno označi, da je jasno razvidno, za katero kopijo gre.

XI.
Evidentiranje zaupnih dokumentov

46. člen

Za evidentiranje zaupnih dokumentov se uporabljajo določila in predpisi pisarniškega poslovanja, še posebno v delu, ki se nanaša na poslovanje z zaupnimi dokumenti.

Evidence zaupnih dokumentov se vodijo ločeno od preostalih evidenc.

V zaupnem dokumentu se pred šifro zadeve označi z veliko tiskano črko »TP«, kar pomeni tajen podatek oziroma »PS«, kar pomeni poslovna skrivnost.

XII.
Arhiviranje zaupnih dokumentov

47. člen

Zaupni dokument se arhivira in čuva skladno s predpisi, ki urejajo arhivsko dejavnost.

Arhivski izvod zaupnega dokumenta je praviloma izvod številka 1 (ena).

48. člen

Pri arhivskem izvodu dokumenta iz prejšnjega člena se lahko hranijo tudi seznami oseb, katerim so bili izvodi izročeni, morebitna dovoljenja za razmnoževanje in seznam oseb, ki so bili z dokumentom seznanjeni.

XIII.
Uničevanje zaupnih dokumentov

49. člen

Za uničenje zaupnih dokumentov se uporabljajo določila, ki urejajo pisarniško poslovanje in arhivsko dejavnost, v delu, ki se nanaša na uničevanje dokumentov, ki so poslovna skrivnost. Komisija, ki uniči zaupni dokument, pošlje zapisnik o uničenju direktorju.

50. člen

Delovno gradivo, ki se uporablja oziroma nastane pri izdelavi zaupnega dokumenta se takoj uniči.

51. člen

Vsako posredovanje poslovne skrivnosti tretjim osebam se vpiše v posebno evidenco, ki jo vodi pooblaščena oseba. Iz evidence mora biti razvidno komu, kaj, kdaj in način prenosa so bili podatki poslovne skrivnosti posredovani.

XIV.
Odgovornost za kršitve

52. člen

Uslužbenec, ki v nasprotju s svojimi dolžnostmi glede varovanja zaupnih podatkov izdaja ali neopravičeno pridobi podatke, ki so tajni podatki po Zakonu o tajnih podatkih, ali poslovna skrivnost, za občino, stori kaznivo dejanje po Kazenskem zakoniku RS in se ga predlaga za pregon.

53. člen

Uslužbenec, ki v nasprotju s svojimi dolžnostmi glede varovanja zaupnih podatkov krši določila tega pravilnika ali drugih aktov občine ali sklepov direktorja, je disciplinsko odgovoren in se ga predlaga v disciplinski postopek oziroma ukrepa v smislu določb sklenjene pogodbe o zaposlitvi.

54. člen

Uslužbenec je odgovoren za nastalo škodo, ki jo povzroči s kršitvijo določb tega pravilnika in je odškodninsko odgovoren in se ga predlaga v odškodninski postopek za povrnitev nastale škode.

XVIII.
Končne določbe

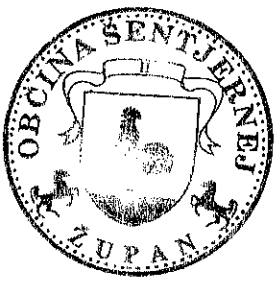
55. člen

Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o varovanju zaupnih in osebnih podatkov (Uradni vestnik Občine Šentjernej, št. 12/2007).

56. člen

Ta pravilnik začne veljati naslednji dan po objavi v Uradnem vestniku Občine Šentjernej, objavi pa se tudi na spletnih straneh Občine Šentjernej.

Številka: 102-02-10/2010
Datum: 01.02.2010



Občina Šentjernej
Župan
Franc Hudoklin