

Na osnovu člana 11 stava 4 tačke 3 Zakona o Policiji Brčko distrikta BiH („Službeni glasnik Brčko distrikta BiH“ brojevi 19/06 i 19/07) i člana 158 stava 1 tačke g) Zakona o policijskim službenicima Brčko distrikta BiH („Službeni glasnik Brčko distrikta BiH“ broj 41/07), šef Policije Brčko distrikta BiH d o n o s i

P R A V I L N I K
O NAČINU OBRADJE TAJNIH PODATAKA
KOJE KORISTI POLICIJA BRČKO DISTRIKTA

DIO PRVI – OPĆE ODREDBE

Član 1
(Predmet Pravilnika)

Ovim pravilnikom se utvrđuju procedure za određivanje i označavanje tajnih podataka, stepena tajnosti i pristupa tajnim podacima u Policiji Brčko distrikta BiH (u daljnjem tekstu: Policiji), mjere i postupci za obradu tajnih podataka, fizičke, tehničke i organizacione mjere i postupci za čuvanje tajnih podataka.

Član 2
(Tajni podatak)

1) Tajnim se smatra podatak čije bi otkrivanje neovlaštenoj osobi, sredstvima javnog informisanja, organizaciji, instituciji, organu ili drugoj državi, odnosno organu druge države, moglo prouzrokovati ugrožavanje integriteta Bosne i Hercegovine (u daljnjem tekstu: BiH), naročito u:

- a) javnoj sigurnosti,
- b) odbrani,
- c) vanjskim poslovima i interesima,
- d) obavještajnim i sigurnosnim interesima BiH,
- e) komunikacionim i drugim sistemima važnih za državne interese, sudstvo, projekte i planove značajne za odbrambeno-sigurnosnu djelatnost i
- f) naučnim, istraživačkim, tehnološkim, privrednim i finansijskim poslovima od važnosti za sigurnost funkcioniranja institucija BiH, odnosno sigurnosnih struktura na svim nivoima državne organizacije BiH.

2) Tajni podatak je činjenica ili sredstvo koje se odnosi na javnu sigurnost, odbranu, vanjske poslove ili obavještajnu i sigurnosnu djelatnost BiH koji je potrebno, u skladu sa odredbama Zakona o zaštiti tajnih podataka (u daljnjem tekstu: Zakon), zaštititi od neovlaštenih osoba i koji je ovlaštena osoba označila oznakom tajnosti. Tajnim podacima smatraju se svi podaci i saznanja koja zaposlenici Policije, u okviru službenog i zakonitog djelovanja, prikupljaju, obrađuju, prosljeđuju ili pohranjuju neovisno o izvornom ili trenutnom raspoloživom izražajnom obliku i koji je ovlaštena osoba označila oznakom tajnosti.

3) Ne može imati karakter tajnosti onaj podatak kojem se tajnost određuje s namjerom prikrivanja izvršenog krivičnog djela, prekoračenja ili zloupotrebe ovlaštenja, s ciljem prikrivanja bilo koje nezakovitosti ili prikrivanja administrativne greške.

Član 3 (Značenje izraza)

- 1) Pojedini izrazi koji se koriste u ovom pravilniku imaju slijedeća značenja:
 - a) "Klasifikacija podataka" je postupak kojim se svakom podatku dodjeljuje odgovarajuće značenje, oznaka osjetljivosti, ugroženosti ili tajnosti;
 - b) "Sigurnosna oznaka" je očima čitljiva oznaka pridodana podatku na osnovu pravnih akata, a koja u postupku nastajanja, pristupa, obrade, primopredaje i prijenosa do pohrane ili uništenja podataka zahtijeva primjenu konkretnih sigurnosnih mehanizama odgovarajuće snage. Sigurnosna oznaka je određena obavezujućom naznakom vrste podataka i naziva tajnosti;
 - c) "Sigurnosni nivo" su mjere i postupci koji se preduzimaju radi osiguranja podataka određenog sigurnosnog nivoa;
 - d) "Zbirke podataka" smatraju se sve zbirke koje se vode na osnovu zakona i podzakonskih akata;
 - e) «Zaposlenik» je policijski službenik, državni službenik i namještenik zaposlen u Policiji.
- 2) Značenja izraza propisanih članom 4 Zakona primjenjuju se i na ovaj pravilnik.

DIO DRUGI- ODREĐIVANJE TAJNOSTI PODATAKA

Član 4 (Ovlaštene osobe za određivanje tajnosti podataka)

- 1) Tajnost podataka, u skladu sa zakonskim uslovima i procedurom određuje ovlaštena osoba.
- 2) U Policiji, ovlaštene osobe za određivanje tajnosti podataka su šef Policije Brčko distrikta BiH (u daljnjem tekstu: šef Policije) i zamjenik šefa Policije.
- 3) Ovlaštene osobe iz stava 2 ovog člana mogu, za određivanje tajnosti podataka, pismeno ovlastiti rukovodioce organizacionih jedinica u okviru kojih se izrađuju i pripremaju tajni podaci i materijali.
- 4) Ovlaštene osobe iz stavova 2 i 3 ovog člana mogu određivati slijedeće stepene tajnosti:
 - a) INTERNO,
 - b) POVJERLJIVO,
 - c) TAJNO.

Član 5 (Prijedlog za određivanje tajnosti podataka)

Svaki zaposlenik Policije obavezan je, da u okviru svojih ovlaštenja, procijeni sigurnosni značaj podataka i predloži ovlaštenim osobama određivanje tajnosti tih podataka ako to ocijene potrebnim.

Član 6 (Procedure za određivanje tajnosti podataka)

U pogledu procedura za određivanje tajnosti podataka shodno se primjenjuju odredbe Zakona.

DIO TREĆI - NAČIN I OBLIK OZNAČAVANJA TAJNIH PODATAKA I STEPENA TAJNOSTI

Član 7 (Način označavanja tajnih podataka)

- 1) Svaki dokument ili medij koji sadrži tajni podatak mora biti označen:
 - a) stepenom tajnosti,
 - b) podacima o organizacionoj jedinici čija je ovlaštena osoba odredila tajnost,
 - c) podacima o ovlaštenoj osobi (ime i prezime, broj i datum ovlaštenja),
 - d) datumom određivanja tajnosti podataka,
 - e) načinom prestanka tajnosti u skladu s odredbama člana 25 Zakona i
 - f) načinom dostavljanja.

- 2) Svaki dokument ili medij koji je označen stepenom tajnosti VRLO TAJNO (ukoliko Policija raspolaže time) ili TAJNO, pored podataka iz stava 1 ovog člana, mora imati i podatke o:
 - a) broju primjeraka dokumenta,
 - b) ukupnom broju stranica dokumenta i
 - c) mogućim priložima i pratećoj dokumentaciji.

- 3) Oznaka tajnosti se mora jasno razlikovati od drugih zapisa, tako da se za pisanje oznaka upotrebljava druga vrsta pisanja, gdje slova ispisana tamnom bojom moraju biti veća od slova ostalih zapisa.

- 4) Pismena ocjena na osnovu koje je određen stepen tajnosti podatka, čuva se kao prilog dokumentu kod organa koji je odredio stepen tajnosti.

- 5) Način i oblik označavanja propisan je na obrascima (prilozi 1 i 2) koji su sastavni dio ovog pravilnika. Ovi obrasci nalaze se u omotu spisa i vidljivi su odmah pri otvaranju omota.

Član 8 (Označavanje tajnih podataka)

- 1) Svaki pisani dokument, uključujući knjige i brošure i njihove reprodukcije, mora imati oznaku stepena tajnosti na vrhu prve strane i vanjske strane prednjih korica ako one postoje ili na vrhu naslovne strane ako je ima. Svaka strana dokumenta mora imati, pored stepena tajnosti, pri dnu naveden i redni broj strane s obzirom na ukupan broj strana dokumenta (npr. 3/9). Ako pisani dokument nema naslovnu stranu, prva strana se smatra kao naslovna, a ako ima naslovnu stranu, prva strana se smatra ona koja se vidi prva kada se otvori naslovna strana.

2) Oznaka na svim drugim dokumentima, odnosno medijima (npr. geografske karte, fotografije, video i audio zapisi, sve vrste elektroničkih zapisa i dr.) koji sadrže tajne podatke, mora biti vidno označena žigom, odštampana, otkucana, napisana, naslikana ili pričvršćena sa etiketom, naljepnicom ili sličnim odgovarajućim sredstvima.

3) Ako se dokument ili medij čuva u bilo kakvom fasciklu, mora biti označen tako da je odmah vidljiv stepen tajnosti tog dokumenta.

4) Prilikom označavanja dokumenata ili medija ne smije doći do uništenja ili oštećenja tajnog podatka, odnosno dokumenta ili medija na kojem se on nalazi, tako da bi on postao neupotrebljiv.

5) Ukoliko dokument ili medij koji je označen stepenom tajnosti ima dodatne dijelove (npr. aneksi, dodaci, grafički prikazi i sl.), označit će se na način kao i osnovni dokument, s tim da stepen tajnosti dodatnih dijelova ne može biti označen većim stepenom tajnosti od osnovnog dokumenta ili medija.

6) Akti kojima se dostavljaju tajni podaci označavaju se istim stepenom tajnosti kao i dokument koji se dostavlja.

Član 9 (Dodatne oznake)

Svaki dokument ili medij, koji je označen stepenom tajnosti VRLO TAJNO (ukoliko Policija raspolaže njima), dodatno je označen crnom linijom debljine najmanje četiri milimetra kojom se podvlači samo stepen tajnosti.

Član 10 (Posebno označavanje)

1) U dokumentu koji sadrži tajne podatke, izuzetno se može označiti svaki pasus sa različitim stepenom tajnosti i to tako da:

- a) se na početku i na kraju svakog pasusa upišu oznake (I), (P), (T) ili (VT),
- b) je dokument, koji sadrži više pasusa različitog stepena tajnosti, označen najvišim stepenom tajnosti pojedinačnog pasusa i
- c) se u prostor za dodatne oznake upišu riječi: "Pasusi su označeni sa različitim stepenom tajnosti".

2) Ovlaštena osoba koja je odredila stepen tajnosti mora u pisanoj ocjeni zapisati i razloge za određivanje različitog stepena tajnosti pojedinačnih pasusa.

Član 11 (Označavanje dodatnih kopija)

1) Svaka dodatna kopija dokumenta ili medija ili njihovog dijela mora biti označena na način propisan u članovima 7 i 8 ovog pravilnika.

2) Kopija iz stava 1 ovog člana dodatno se označava:

- a) oznakom "kopija originala",
- b) rednim brojem kopije,

- c) brojem i datumom evidencije o umnožavanju,
- d) oznakom organizacione jedinice i
- e) potpisom službenika koji je izvršio umnožavanje.

3) Svaka umnožena stranica mora u gornjem desnom uglu imati otisnutu oznaku KOPIJA ORIGINALA tako da otisak ne prekriva sadržaj dokumenta.

4) Način i oblik označavanja propisan je na obrascima (prilozi 3 i 4) koji su sastavni dio ovog pravilnika.

Član 12 **(Oznaka promjene stepena tajnosti)**

1) Ukoliko ovlaštena osoba donese odluku o promjeni stepena tajnosti dokumenta ili medija, o njemu će pismeno obavijestiti sve zakonske korisnike. Dokumentu ili mediju, kojem se mijenja stepen tajnosti će se priložiti odluka o promjeni stepena tajnosti.

2) Ako je dokument ili medij poslije promjene stepena tajnosti još uvijek označen sa jednim od stepena tajnosti, potrebno je uraditi slijedeće:

- a) prekrížiti originalnu oznaku,
- b) dokument ili medij označiti na posebnom listu sa odgovarajućom oznakom iz člana 7 ovog pravilnika, koja uključuje i navođenje broja i datuma pismene obavijesti o promjeni stepena tajnosti i
- c) staviti datum i potpis ovlaštene osobe organizacione jedinice koja je oznaku prepravila.

3) Na dokumentu ili mediju potrebno je precrtati sve stare oznake stepena tajnosti i iznad ili ispod stare oznake upisati novi stepen tajnosti.

4) Ukoliko je došlo do prestanka tajnosti dokumenta on se označava na način da se prekríži oznaka stepena tajnosti i ispod toga upišu riječi "PRESTANAK TAJNOSTI", datum prestanka i potpis ovlaštene osobe.

Član 13 **(Ispravka tajnog podatka)**

1) Ukoliko je dio teksta u dokumentu pogrešno upisan, ispravka se vrši na posebnom listu koji je sastavni dio dokumenta, a sadrži konkretne podatke o ispravci.

2) Na sredini donjeg dijela posebnog lista upisuje se riječ "ISPRAVKA" čija su slova veća od slova ostalog dijela teksta.

Član 14 **(Stepeni tajnosti)**

1) Tajni podaci iz člana 2 ovog pravilnika imaju jedan od slijedećih stepena tajnosti:

- a) VRLO TAJNO određuje se za podatke čije bi neovlašteno otkrivanje ugrozilo integritet BiH i nanijelo državi nepopravljivu štetu,
- b) TAJNO se određuje za podatke čije bi neovlašteno otkrivanje nanijelo izuzetne štetne posljedice po sigurnosne, političke, ekonomske ili druge interese BiH,

- c) POVJERLJIVO se određuje za podatke čije bi neovlašteno otkrivanje nanijelo štetu sigurnosti ili interesima BiH i
- d) INTERNO se određuje za podatke čije bi neovlašteno otkrivanje moglo štetiti djelovanju BiH, Brčko distrikta ili organa, organizacija i institucija na ostalim nivoima državne organizacije BiH.

Član 15 **(Stepen tajnosti TAJNO)**

1) Stepenom tajnosti TAJNO, na način propisan ovim pravilnikom, označavaju se podaci i svi izvori podataka koji se odnose na planiranje i provedbu mjera i radnji iz glave IX Zakona o krivičnom postupku BiH i Zakona o krivičnom postupku Brčko distrikta BiH, Zakona o zaštiti svjedoka pod prijetnjom i ugroženih svjedoka, Zakona o programu zaštite svjedoka u BiH, sa posebnim osvrtom na slijedeće:

- a) Pojedinačni raspored policijskih službenika unutar Policije vezani za posebne operacije ili akcije,
- b) Podaci o organizaciji, planovima, sredstvima i sistemu veza u Policiji;
- c) Kartografske publikacije i crteži koji sadrže operativne podatke;
- d) Planovi rada o posebnim operacijama i akcijama, kriminalističko-obavještajni izvještaji, informacije, analize i procjene pojedinih predmeta;
- e) Podaci o osobama koje se vode u operativnim evidencijama Policije;
- f) Podaci o izvorima obavještenja i prikupljenih podataka, odnosno saznanja Policije;
- g) Podaci dobijeni od informanata i preko krimolovaca, kao i identitet osobe koja daje podatke;
- h) Planovi postupanja u vanrednim situacijama;
- i) Instruktivni i drugi akti vezani za podatke ove vrste i stepena tajnosti.

2) Oznakom iz stava 1 ovog člana označavaju se podaci i svi izvori podataka o službenicima i to:

- a) koji provode mjere kojima se privremeno ograničavaju ustavna prava građana,
- b) koji obavljaju zadatke prikrivenog istražitelja ili pouzdanika, odnosno koji učestvuju u simuliranom otkupu predmeta, te simuliranim davanjima ili primanjima otkupnine,
- c) koji provode mjere osiguranja šticećenih osoba, objekata i prostora i
- d) koji su pripadnici Jedinice policije za podršku.

Član 16 **(Stepen tajnosti POVJERLJIVO)**

1) Stepenom tajnosti POVJERLJIVO označavaju se podaci i svi izvori podataka koji se odnose na:

- a) Planove Policije za obezbjeđenje određenih osoba i objekata;
- b) Podatke o aktivnostima određenih organizacionim jedinicama i podaci o policijskim službenicima kao izvršiocima;
- c) Podatke o finansijskim sredstvima raspoređenim za posebne namjene;

- d) Podatke dobijene sistemom videonadzora;
- e) Instruktivne i druge akte vezana za podatke ove vrste i stepena tajnosti.

2) Znakom iz stava 1 ovog člana označavaju se podaci i svi izvori podataka koji se vode u zbirka DNK uzoraka i daktiloskopskih otisaka, te svih drugih specifičnih, prepoznatljivih obilježja kojima se utvrđuje ili je utvrdiva ličnost ili identitet fizičke osobe.

Član 17 (Stepen tajnosti INTERNO)

Stepenom tajnosti INTERNO označavaju se podaci i svi izvori podataka i to:

- a) Vježbe policijskih službenika Policije;
- b) Objekti u kojima se čuva oprema i druga materijalna sredstva za potrebe Policije;
- c) Opremanje naoružanjem, municijom, opremom i drugim materijalno-tehničkim sredstvima;
- d) Personalni dosjei zaposlenih;
- e) Dokumenti koji sadrže lične podatke;
- f) Planovi i programi posebnog stručnog osposobljavanja zaposlenih u Policiji;
- g) Instruktivni i drugi akti vezani za podatke ove vrste i stepena tajnosti.

Član 18 (Međunarodni termini za stepene tajnosti)

Međunarodni termini za stepene tajnosti su:

- a) stepenu «VRLO TAJNO» odgovara termin «TOP SECRET»,
- b) stepenu "TAJNO" odgovara termin "SECRET",
- c) stepenu "POVJERLJIVO" odgovara termin "CONFIDENTIAL" i
- d) stepenu "INTERNO" odgovara termin "RESTRICTED".

DIO ČETVRTI - SIGURNOSNA PROVJERA I PRISTUP TAJNIM PODACIMA

Član 19 (Predmet sigurnosnih provjera)

- 1) Zaposlenici Policije, kao i osobe koje se prijavljuju za radno mjesto u Policiji, bit će predmet osnovne sigurnosne provjere u skladu s postupkom za izdavanje dozvole za pristup tajnim podacima POVJERLJIVO.
- 2) U pogledu sigurnosne provjere shodno se primjenjuju odredbe Zakona i Pravilnika o listi organa čiji su službenici i osobe koje se prijavljuju za rad predmet osnovnog sigurnosnog provjeravanja.

Član 20 (Pristup tajnim podacima)

- 1) Pravo pristupa tajnim podacima kojima rukuje Policija imaju zaposlenici Policije koji su dobili dozvolu od šefa Policije i to samo pri obavljanju dužnosti ili u okviru radnih zadataka.

2) Pravo pristupa za zaposlenike iz stava 1 ovog člana odnosi se samo na tajne podatke određene u dozvoli.

3) Niko ne smije tražiti tajni podatak prije i u većem obimu nego što je potrebno za obavljanje dužnosti ili radnih zadataka.

4) U pogledu pristupa tajnim podacima kojima rukuje Policija shodno se primjenjuju odredbe Zakona.

Član 21 **(Pristup tajnim podacima druge države, međunarodne ili regionalne organizacije)**

U pogledu načina izdavanja dozvole za pristup tajnim podacima druge države, međunarodne ili regionalne organizacije kojima rukuje Policija shodno se primjenjuju odredbe Zakona i Pravilnika o načinu izdavanja dozvole za pristup tajnim podacima druge države, međunarodne ili regionalne organizacije.

DIO PETI - ČUVANJE TAJNIH PODATAKA

Član 22 **(Cilj mjera čuvanja)**

1) Cilj mjera neposrednog fizičkog čuvanja tajnih podataka, osiguravanja prostora i objekata (fizičke mjere), mjera čuvanja tajnih podataka, osiguravanja prostorija ili objekata sa tehničkim sredstvima u skladu sa ovim pravilnikom (tehničke mjere), te mjera postupanja organizacionih jedinica Policije u pripremanju, čuvanju i uništavanju tajnih podataka (organizacione mjere) je onemogućavanje pristupa, odnosno otkrivanja tajnih podataka neovlaštenim osobama.

2) Prilikom osiguravanja tajnih podataka druge države ili međunarodnih organizacija, pored ili umjesto mjera propisanih ovim pravilnikom, mogu se izvoditi i druge mjere osiguravanja određene međunarodnim ugovorima ili prihvaćenim međunarodnim obavezama.

Odjeljak A: Fizičke mjere zaštite

Član 23 **(Faktori pri određivanju mjera zaštite)**

1) Svi objekti, zgrade, uredi, sobe i drugi prostori Policije u kojima se arhiviraju tajni podaci i gdje se njima rukuje, trebaju biti zaštićeni odgovarajućim mjerama fizičke zaštite. Pri odlučivanju o stepenu potrebne fizičke sigurnosne zaštite, u obzir će se uzeti slijedeći faktori:

- a) nivo povjerljivosti i kategorija informacije,
- b) količina i oblik informacija (štampane na papiru, na medijima za kompjutersko pohranjivanje),
- c) sigurnosna provjera i zaposlenici Policije koji trebaju znati informacije i
- d) kako će se arhivirati informacije.

2) Mjere fizičke zaštite će biti tako osmišljene da:

- a) spriječe nedozvoljen ili nasilan upad od neovlaštene osobe,

- b) odvrate, spriječe i otkriju radnju neovlaštene osobe,
- c) omoguće selekciju zaposlenika Policije u pogledu pristupa tajnim podacima i
- d) omoguće otkrivanje i postupanje u svim slučajevima ugrožavanja sigurnosti što je prije moguće.

Član 24 **(Sigurnosno područje)**

1) Tajni podaci stepena INTERNO se mogu obrađivati u administrativnom području. Tajni podaci stepena tajnosti POVJERLJIVO ili većeg stepena se mogu obrađivati i čuvati samo u određenom, vidljivo označenom prostoru (u daljnjem tekstu: sigurnosno područje), koje je, shodno načinu obrade tajnih podataka, uvršteno u sigurnosno područje I ili II stepena.

2) Sigurnosno područje I stepena je označen prostor u kojem se mogu obrađivati tajni podaci stepena POVJERLJIVO ili višeg stepena tajnosti, tako da već sam ulazak u sigurnosno područje znači dostup do tih podataka. U sigurnosnom području I stepena se izvode najmanje slijedeći sigurnosni postupci i mjere:

- a) sistem ulaznog nadziranja, koji osigurava potpuni nadzor nad ulazom odnosno izlazom osoba i vozila u to područje, dozvoljava ulaz samo osobama, koje imaju odgovarajuću dozvolu za pristup do tajnih podataka i koje su zaposlene u tom području, odnosno imaju posebne dozvole za ulazak u to područje,
- b) vođenje evidencija tajnih podataka, s kojim se osoba upozna već prilikom samog ulaska u sigurnosno područje,
- c) zabrana unosa bilo kakvih mehaničkih, elektroničkih i magnetno-optičkih sastavnih dijelova, kojima bi bilo moguće neovlašteno snimiti, odnijeti ili prenijeti tajne podatke,
- d) neposredno i neprekidno fizičko osiguranje sigurnosnog područja, koje se može na podlozi ocjene ugroženosti dopuniti ili nadomjestiti s elektroničkim sistemom za protivprovalno osiguranje sigurnosnog područja, čiji je alarmni sistem povezan sa jedinicom odgovornom za intervenciju prilikom alarma (dežurna služba – operativni centar), vrijeme intervencije mora biti kraće od sedam minuta,
- e) prilikom nadomještanja fizičkog osiguranja sistemom tehničkog osiguranja taj sistem mora osigurati cjelovit nadzor sigurnosnog područja, koje mora biti nadgledano iz dežurne službe – operativnog centra i sistem mora imati osigurano rezervno napajanje i
- f) po završenom radnom vremenu prostori se pregledaju.

3) Sigurnosno područje II stepena je označen prostor u kojem se tajni podaci stepena POVJERLJIVO ili višeg stepena obrađuju na taj način, da sam ulazak i kretanje u tom području još ne omogućava pristup do tih podataka. U sigurnosnom području II stepena se izvode najmanje sljedeći postupci i mjere:

- a) sistem ulaznog nadziranja koji ulazak u to područje dozvoljava samo osobama, koje imaju dozvolu za pristup tajnim podacima odgovarajućeg stepena tajnosti i moraju u područje ući zbog izvršavanja radnih zadataka,
- b) takva organizacija rada, kojom se osigurava, da će osobe, koje rade u sigurnosnom području, imati pristup samo do onih tajnih podataka, koji su im potrebni za izvršavanje radnih zadataka i to do onog stepena tajnosti, za koji imaju dozvolu,

- c) sistem nadziranja kretanja, kojim se osigurava, da druge osobe ulaze u sigurnosno područje samo u pratnji zaposlene osobe ili uz izvođenje odgovarajućeg oblika nadzora, kojim se osigurava da će osoba ulaziti samo u dijelove područja povezane sa razlogom ulaska i ako je to potrebno upoznat će samo sa onim tajnim podacima koji su povezani sa razlogom ulaska, i to do onog stepena tajnosti, za koji ima dozvolu,
- d) unošenje bilo kakvih mehaničkih, elektroničkih i magnetno-optičkih sastavnih dijelova, kojima bi bilo moguće tajne podatke neovlašteno snimiti, odnijeti ili prenijeti, je dozvoljeno, ali sva oprema mora biti isključena, svaku njenu upotrebu odobrava osoba odgovorna za sigurnost područja i
- e) po završenom radnom vremenu se sigurnosno područje osigurava sistemom, fizičkog ili protivprovalnog osiguravanja, odnosno povremenim fizičkim pregledima prostora, određenih u planu čuvanja.

4) Oko sigurnosnog područja I ili II stepena ili na putu koji vodi u takvo sigurnosno područje uspostavlja se administrativno područje koje može zahvatiti sve službene prostorije objekta Policije. Za takvo područje određuje se lokacija na kojoj Policija može nadzirati ulaznje, odnosno kretanje osoba i vozila. U administrativnom području se mogu čuvati i obrađivati samo tajni podaci stepena INTERNO, a sigurnosnim postupcima i mjerama se mora osigurati, da pristup do tih podataka imaju samo osobe, koje su pismenom izjavom potvrdile da su upoznate sa propisima koji uređuju obrađivanje tajnih podataka i koje se moraju s tim podacima upoznati zbog izvršavanja radnih zadataka.

5) Za ulazak u sigurnosno područje i stepena osobi se izdaje posebna dozvola ovlaštene osobe iz člana 4 stavova 2 i 3 ovog pravilnika.

6) Ulazak osoba u sigurnosno područje i njihov izlazak te prilaz vozila moraju biti pod nadzorom. Svi ulazi i izlazi se moraju evidentirati.

Član 25 (Sigurnosna propusnica)

1) Sve osobe koje se kreću u sigurnosnom području I ili II stepena moraju imati na vidljivom mjestu zakačenu sigurnosnu propusnicu za ulazak i kretanje u sigurnosnom području I ili II stepena koja se razlikuje shodno statusu osobe (propusnica za zaposlene, posjetioce, tehnički personal i sl.). Policija će voditi evidenciju o izdatim sigurnosnim propusnicama.

2) Propisom se može odrediti kad neke osobe u sigurnosnom području I ili II stepena ne moraju nositi na vidljivom mjestu sigurnosnu propusnicu.

3) Odluku o izgledu sigurnosne propusnice i njenoj tehničkoj izradi donosi šef Policije.

Član 26 (Određivanje sigurnosnog i administrativnog područja)

1) Određivanje stepena klasifikacije sigurnosnih i administrativnih područja u Policiji i stepena njihove zaštite odgovarat će značaju podataka sa sigurnosnog aspekta koje je

potrebno zaštititi.

2) Šef Policije, na prijedlog zamjenika šefa Policije, odlukom određuje sigurnosna i administrativna područja sa odgovarajućom sigurnosno-tehničkom opremom ugrađenom u sigurnosno područje, kao i postupke i mjere osiguranja sigurnosnog područja.

Član 27 (Označavanje sigurnosnih i administrativnih područja)

1) Osoba koja bude stupila u sigurnosno područje mora biti o tome nedvojbeno i jasno obavještena prije nego stupi u to područje.

2) Obavještenje iz stava 1 ovog člana mora sadržavati vidan natpis: " Policija Brčko distrikta - SIGURNOSNO PODRUČJE" - II odnosno I stepena, a mogu im biti dodata i druga obavještenja povezana sa sigurnosnim postupcima i mjerama koje se izvode u sigurnosnom području.

3) Za označavanje administrativnog područja nije potrebno posebno obavještenje iz stava 2 ovog člana, ali to područje odnosno zgrada ili okoliš u kojem je područje, mora biti označeno tablama na kojima je napisan naziv Policije te obavještenje o nadzoru pristupa i kretanja, ako se ono izvodi.

4) Izuzetno, kad to zahtijevaju posebne okolnosti, šef Policije može u odluci o određivanju sigurnosnog područja propisati da se sigurnosno područje ne označi sa obavještenjem iz stava 2 ovog člana, odnosno da se označi na način koji javnosti ne otkriva da je to objekat Policije.

Član 28 (Nadzor ulaza i izlaza)

1) Ulazak zaposlenika u sigurnosna i administrativna područja Policije nadzire se provjerom identiteta osoba koje ulaze. Fizički nadzor ulaska može dopunjavati sistem automatskog prepoznavanja identifikacijskih kartica.

2) Prije ulaska drugih osoba u sigurnosno i administrativno područje Policije, osoba koja nadzire ulazak u sigurnosno područje mora provjeriti njihov identitet i razlog ulaska, kao i ispunjavanje drugih uslova za ulazak u sigurnosno područje.

3) Drugim osobama kojima se dozvoljava ulazak u sigurnosno područje izdaje se sigurnosna propusnica kojom se dozvoljava kretanje u sigurnosnom području i daje im se do znanja da je njihovo kretanje nadzirano i evidentirano.

4) Podaci iz stavova 2 i 3 ovog člana upisuju se u evidenciju ulaska i kretanja u sigurnosnom području Policije.

5) U planu čuvanja sigurnosnog područja moraju biti predviđene mjere i postupci pooštrenog nadzora, odnosno ograničenje ulaska i kretanja u sigurnosnom i administrativnom području kad to diktira ocjena ugroženosti ili promijenjene sigurnosne prilike.

6) U prostore koji su posebno namijenjeni za rad sa strankama, mogu posjetio i druge osobe u pratnji stranke ulaziti i izlaziti u prisustvu zaposlenika Policije bez provjeravanja identiteta i vođenja evidencija onih koji ulaze.

7) Osoblje koje je pod ugovorom (uključujući pomoćno tehničko osoblje za održavanje i čišćenje) morat će ili biti podvrgnuto sigurnosnoj provjeri za odgovarajući stepen tajnosti ili cijelo vrijeme biti pod pratnjom. Tehničari za automatsku obradu podataka trebaju biti podvrgnuti sigurnosnoj provjeri za najveći stepen tajnosti podataka koji se obrađuju na sistemu.

Član 29 (Osiguranje opreme)

1) Fotokopirne mašine, telefaksi i druge naprave za obradu tajnih podataka, koji su postavljeni u sigurnosnom području moraju biti osigurani tako da ih mogu upotrebljavati zaposlenici koji su ovlašteni za rad tim aparatima.

2) Sva elektronička oprema za obradu podataka, uključujući aparate za umnožavanje, telefakse, računare i slično, bit će označena sa odobrenom naljepnicom koja prikazuje njihovu prikladnost za obradu povjerljivih informacija.

Član 30 (Obrada tajnih podataka izvan sigurnosnog područja)

1) Tajni podaci se mogu obrađivati izvan sigurnosnog područja, ako je prostor ili područje, u kojem se tajni podatak obrađuje fizički ili tehnički osiguran, a pristup do prostora je pod nadzorom. Zaposlenik Policije koji obrađuje tajni podatak izvan sigurnosnog područja, mora imati tajni podatak cijelo vrijeme pod nadzorom. Po okončanoj obradi, tajni podatak se vraća u sigurnosno područje.

2) Kada se mora, tajni podatak stepena tajnosti POVJERLJIVO ili višeg stepena tajnosti, radi izvođenja tačno određenog naloga, obrađivati izvan prostora Policije, rukovodilac organizacione jedinice mora izraditi nacrt mjera i postupaka za osiguranje tajnog podatka s obzirom na njegov stepen tajnosti. Mjere i postupci moraju biti saglasni sa mjerama i postupcima koji su propisani za posebno sigurnosno područje.

3) Svako iznošenje ili unošenje tajnog podatka stepena tajnosti POVJERLJIVO i višeg stepena izvan sigurnosnog područja se evidentira. Zaposlenik Policije koji preuzme tajni podatak, potvrđuje to sa vlastoručnim potpisom, čime preuzima odgovornost za sigurnost tajnog podatka.

Odjeljak B: Tehničke mjere zaštite

Član 31 (Opće odredbe)

Tehničke mjere zaštite tajnih podataka obuhvataju mjere čuvanja, osiguravanja prostorija ili objekata Policije sa tehničkim sredstvima.

Član 32 (Izgradnja objekata)

1) Pri izgradnji i uređenju objekata Policije mora se voditi računa da prostori u kojima će se koristiti, obrađivati, arhivirati ili uništavati tajni podaci sigurnosnog područja I stepena budu na prvom spratu ili višim spratovima građevinskog objekta sa neprozirnim zavjesama na prozorima koje onemogućavaju pogled u unutrašnjost, te sa sigurnosnim zvučno izoliranim ulaznim vratima s mehanizmom za samozatvaranje, bez ostakljenja iznad vrata.

2) Ukoliko građevinski objekat Policije nema više spratova ili iskoristiv prostor na višim spratovima, izuzetno, prostor može biti u prizemlju, ispunjavajući sve uslove iz stava 1 ovog člana uz dodatak sigurnosnih metalnih rešetki na prozorima.

3) Ako je prostor iz stava 1 ovog člana u potkrovlju građevinskog objekta Policije onda ne smije imati krovne prozore.

Član 33 (Prostorije)

1) Prostori u koje se postavljaju telefonske centrale i druga telekomunikacijska oprema za objedinjavanje sveukupnog telekomunikacijsko-informatičkog prometa kao i prostori u kojima se postavljaju centralni poslužitelji informatičkih sistema (serveri) moraju biti u prizemlju bez prozora ili sa sigurnosnim metalnim rešetkama na prozorima i bez mogućnosti otvaranja prozora te s potpuno zatamljenim staklima, koja onemogućavaju pogled u unutrašnjost prostorije.

2) Prostori u kojima se postavljaju serveri i telekomunikacijska oprema moraju zadovoljavati ISO standarde.

3) Ukoliko građevinski objekat Policije nema iskoristiv prostor u prizemlju, izuzetno se može koristiti i prostor na višim spratovima ispunjavajući sve uslove iz stava 1 ovog člana.

4) Ukoliko se određeni prostor nalazi u potkrovlju, prostor iz stava 1 ovog člana ne smije imati krovne prozore.

Član 34 (Prostorije za smještaj sigurnosne opreme)

Prostorije za smještaj sigurnosne opreme u svim objektima Policije moraju biti opremljene:

- a) jednim od pristupnih sigurnosno-zaštitnih mehanizama na ulaznim vratima, s mogućnošću arhiviranja podataka o ulasku u prostor kako bi se pristup takvim prostorijama mogao ograničiti i nadzirati,
- b) opremom za sigurno arhiviranje i čuvanje predmeta i dokumenata,
- c) energetske priključkom na centralno neprekidno i agregatsko napajanje i
- d) sigurnosnim mehaničkim sistemom za zaključavanje s ograničenim brojem ključeva bez mogućnosti umnožavanja ili tome odgovarajuća odvojena automatizirana i manualna rješenja.

Član 35 (Računari)

1) Računari koji se koriste u procesu obrade tajnih podataka, moraju imati sljedeće funkcionalne module:

- a) modul za sigurno prijavljivanje na računar koji će jednoznačno utvrditi identitet osobe i omogućiti pristup samo dokumentima sigurnosnog nivoa koje je odobreno i zapisati sve radnje izvršene od tog korisnika u računar posebne namjene (Log.Server) i
- b) modul za onemogućavanje neovlaštenog kopiranje podataka sa i na prijenosne magnete ili optičke medije-modul kontinuiranog osiguranja i zaštite od djelovanja računarskih virusa i neovlaštenih programa i upada neovlaštenih korisnika.

2) Računari koji se koriste u procesu obrade tajnih podataka uz mehanizme navedene u stavu 1 ovog člana moraju sadržavati i kriptografske mehanizme koji će osigurati tajnost i integritet podataka na silikonskim (RAM, ROM, flash...), magnetnim (HD, floppy, traka...) i optičkim (CD, DVD...) medijima u slučaju da su oni neovlašteno korišteni.

Član 36 (Povezivanje računara)

1) Međusobno povezivanje računara koji se koriste u procesu obrade tajnih podataka u mrežu dozvoljeno je samo:

- a) ako za to postoji opravdani razlog,
- b) ako postoji pisana saglasnost rukovodioca organizacionih jedinica Policije, odgovornih za sigurnost informacija pohranjenih na datim računarima i
- c) ako su računari i korisnici računara istih sigurnosnih nivoa.

2) Umnožavanje ili pohranjivanje informacija sa jednog na drugi informacijsko-komunikacijski sistem različite sigurnosne klasifikacije (npr. umnožavanje jednog dokumenta BEZ SIGURNOSNE KLASIFIKACIJE sa informacijsko-komunikacijskog sistema stepena klasifikacije TAJNO na informacijsko-komunikacijski sistem BEZ SIGURNOSNE KLASIFIKACIJE uz pomoć diskete) bit će dozvoljeno samo u okolnostima koje su bitne u operativnom smislu, primjenjujući postupke koje je odredila Policija.

3) Povezivanje računara koji se koriste u procesu obrade tajnih podataka različitih sigurnosnih nivoa dozvoljeno je samo uz obaveznu primjenu sigurnosnog rješenja koje će onemogućiti prijenos podataka sa računara višeg sigurnosnog nivoa na računar nižeg sigurnosnog nivoa.

Član 37 (Preduslovi za korištenje računarske opreme)

1) Samo odobreni hardveri će se koristiti ili priključivati na informacijsko-komunikacijski sistem. Bez prethodnog odobrenja Policije, neće se vršiti nikakve izmjene na hardveru koje bi utjecale na sigurnosni profil nekog sistema.

2) Za svaki računar koji se koristi u procesu obrade tajnih podataka, moraju se odrediti potrebni servisi i programski moduli, a svi nepotrebni moduli i servisi moraju biti uklonjeni.

3) Komponente i sredstva komunikacija koja zadržavaju podatke stepena klasifikacije

TAJNO i iznad (ukoliko Policija raspolaže sa istim) potrebno je evidentirati, zaštititi i pregledati na sličan način kao i papirnu dokumentaciju istog stepena klasifikacije. Za fiksne hard drajvove stepena klasifikacije **TAJNO** ili iznad (ukoliko Policija raspolaže sa istim), kućište računara (kućište centralne jedinice za obradu podataka) u kojem je drajv smješten bit će označeno sa sigurnosnom klasifikacijom, dok će se serijski broj kućišta računara koristiti za materijalnu evidenciju.

4) Svi potrebni servisi i softverski moduli moraju biti provjereni da ne sadrže dokumentovane ili nedokumentovane procedure ili funkcije koje mogu smanjiti sigurnost sistema.

Član 38 (Informatičko osoblje)

1) Svaki sistem informatičke tehnologije (informacijsko-komunikacijski sistem) posluživat će zaposlenici Policije za osiguranje odgovarajuće strukture za upravljanje sigurnosnim mjerama radi sprovođenja i održavanja mjera zaštite informacijsko-komunikacijskog sistema koje će se primjenjivati na datoj lokaciji. Zaposlenici Policije za osiguranje informacijsko-komunikacijskog sistema bit će uključeni u organizaciju za upravljanje sigurnosnim mjerama. Za veći informacijsko - komunikacijski sistem ili specifična područja imenovat će se dodatni zaposlenici kao oficiri za sigurnost područja kompjuterskih terminala (TASO) ili oficiri za sigurnost lokacije radi izvršenja dužnosti zaštite informacijsko-komunikacijskog sistema. Oficir za sigurnost područja kompjuterskih terminala bit će odgovoran za svakodnevno rukovođenje mjerama zaštite rada informacijsko-komunikacijskog sistema u njegovom području odgovornosti. Oficir za sigurnost lokacije bit će odgovoran za sprovođenje i održavanje mjera zaštite informacijsko-komunikacijskog sistema koje će se primjenjivati na lokaciji.

2) Odgovornost administratora i rukovodioca sistema je da pruže savjete zaposlenicima Policije za osiguranje informacijsko-komunikacijskog sistema i da ih uključe u sve aktivnosti i odluke u vezi sa sigurnošću.

3) Obavezno je provođenje separacije poslova između sigurnosnog i općeg administratora za sve IKT uređaje uključene u obradu tajnih podataka.

4) Svaki IKT uređaj uključen u obradu tajnih podataka mora imati imenom i prezimenom zaduženog administratora u skladu s odredbom stava 1 ovog člana koji su odgovorni za sigurnost, pouzdanost i raspoloživost predmetne opreme.

Član 39 (Obaveze u radu s informatičkom opremom)

1) Odjeljenje za informatiku i komunikacije Policije, formulirat će politiku za ograničavanje broja aktivnih pomoćnih drajvova i uređaja u područjima odgovornosti. Prilikom formuliranja ovih sigurnosnih politika, primijenit će se sljedeći uslovi:

- a) Samo oni uređaji za čitanje disketa koji su bitni za zadovoljenje operativnih potreba bit će aktivirani na informacijsko-komunikacijskom sistemu koji obrađuje podatke stepena klasifikacije **POVJERLJIVO** i iznad. Kao rukovodeći princip, isključivo jedan uređaj za čitanje disketa bit će aktiviran u svakom

- odjeljenju, odsjeku ili drugoj jedinici Policije. Gdje god je to moguće, ovi aktivirani drajvovi nalazit će se u administrativnom odjeljenju odjeljenja, odsjeka ili druge jedinice Policije.
- b) CD-ROM (i DVD) drajvovi bit će omogućeni samo ako je omogućena sigurnosna funkcionalnost formalno procijenjenog operativnog sistema kako bi se spriječilo da korisnik unosi izvršnu šifru u informacijsko - komunikacijski sistem.
 - c) CD čitač/pisač, Zip/Jazz drajvovi i drajvovi za trake koristit će se samo u administrativnim područjima (informacijsko-komunikacijskog sistema u kojima će kreiranje ovakvih sredstava za pohranjivanje velike količine podataka da vrši imenovano i kvalificirano osoblje koje će biti posebno informirano o ispravnim procedurama kojih se treba pridržavati).
 - d) Na informacijsko-komunikacijskom sistemu koristit će se samo uređaji USB za pohranjivanje velike količine podataka koji su pribavljeni zvaničnim putem. Uređaji USB za pohranjivanje velike količine podataka neće se koristiti na informacijsko-komunikacijskim sistemima stepena klasifikacije "VRLO TAJNO" (ukoliko Policija raspolaže sa istima) ili onima posebne vrste. Svi uređaji USB za pohranjivanje velike količine podataka trebaju se označiti i manipulirati u skladu sa važećim stepenom tajnosti podataka koji su ikad bili sadržani na ovom uređaju ili važećim stepenom klasifikacije i informacijsko-komunikacijskog sistema na koji su bili priključeni (koji god da je veći). Krađu, gubitak ili sumnju o kompromitiranju uređaja USB za pohranjivanje velike količine podataka potrebno je odmah prijaviti. Za informacijsko-komunikacijske sisteme stepena klasifikacije TAJNO, samo oni terminali koji se nalaze u području koje obezbjeđuju policijski službenici (obezbjeđenje 24 sata, sedam dana u sedmici) treba da imaju mogućnost korištenja uređaja USB za pohranjivanje velike količine podataka.
 - e) Priključivanje digitalnih kamera na informacijsko-komunikacijske sisteme sa sigurnosnom klasifikacijom ograničit će se na područja / terminale koji su u operativnom smislu bitni u sredinama koje su pod nadzorom kao što su npr. administrativni uredi, a zaposlenici koji su odgovorni za uploading (prijenos podataka sa računara na server) odnosno downloading (prijenos podataka sa servera na računar) primit će posebna uputstva za ovu radnju.
 - f) Svaki softver na informacijsko-komunikacijskom sistemu operacija održavat će se pod strogom konfiguracijskom kontrolom. Na informacijsko - komunikacijskim sistemima koristit će se isključivo softveri koji su nabavljeni i za koje je dozvola izdata zvaničnim putem. Osigurat će se da sve softverske kopije budu evidentirane, kontrolirane i pohranjenje u svrhu sigurnosne kopije u skladu sa odobrenim procedurama i po mogućnosti, označene sa odgovarajućom sigurnosnom klasifikacijom.
 - g) Ovlašteni korisnici informacijsko-komunikacijskog sistema neće dozvoliti nikome drugom, uključujući druge ovlaštene korisnike, da ostvare pristup informacijsko-komunikacijskom sistemu pomoću njihove lozinke ili korisničkog identiteta. Grupni korisnički računi neće se koristiti na informacijsko-komunikacijskim sistemima koji obrađuju informacije stepena klasifikacije POVJERLJIVO ili iznad.
 - h) Sistem administrator obavezan je izraditi plan pravljenja sigurnosnih kopija (Backupa) i provjeravati njegovu efikasnost za sve podatke koji se nalaze na računarima pod njegovom administrativnom kontrolom.

2) Svaki informacijski sistem mora imati servere u mrežnom operativnom centru,

najmanje dva na geografski odvojene lokacije, između kojih se vrši stalna replikacija podataka kako bi se u slučaju kvara, poplave, požara i drugih prirodnih katastrofa osigurao neprekidan rad sistema.

3) Procedure za tehničko održavanje informacijsko-komunikacijskog sistema i opreme bit će precizno definirane kako bi se osiguralo da pomoćno tehničko osoblje koje nije prošlo sigurnosnu provjeru ne može ostvariti pristup povjerljivim informacijama. Održavanje vrši pomoćno tehničko osoblje koje je prošlo sigurnosnu provjeru na odgovarajući način ili, izuzetno, osoblje koje nije prošlo sigurnosnu provjeru ali je pod stalnim nadzorom tehničkih stručnjaka ili osoblja koje je prošlo odgovarajuću sigurnosnu provjeru. Vodit će se evidencija o svakom tehničkom održavanju informacijsko-komunikacijskog sistema i opreme.

Član 40 (Obaveze korisnika)

- 1) Svaki korisnik, zaposlenik Policije, pojedinačno je odgovoran da:
 - a) se pobrine da bude propisno obučen za vršenje neophodnih radnji na sistemu,
 - b) se pobrine da pročita, razumije i pridržava se svih sigurnosnih procedura o sigurnom radu njihovih zasebnih informacijsko-komunikacijskih sistema i
 - c) prijavi svaki sigurnosni incident ili neobičan događaj koji se može opaziti tokom rada informacijsko-komunikacijskog sistema.

- 2) Zaposlenici Policije koji koriste informatičku opremu ili informatički sistem za obradu tajnih podataka obavezni su:
 - a) svaki pristup obavljati iz službenih razloga, bez negativnog utjecaja na službenu produktivnost u toku radnog vremena i uz obavezno evidentiranje korištenja i zatečenog stanja,
 - b) odgovorno i redovno obavljati svaku dokumentiranu razmjenu tekstova, zvučnih i slikovnih zapisa, zbirki podataka te računarskih programa posredstvom informatičkog sistema i
 - c) aktivirati sigurnosno-zaštitne mehanizme računarske jedinice od mogućeg djelovanja računarskih virusa prilikom predaje ili prijema bilo kojeg spisa.

Član 41 (Obaveze kod promjene radnog statusa)

U slučaju kada zaposleniku Policije, koji je imao pristup tajnim podacima, prestaje radni odnos ili kada se raspoređuje na rad u drugu organizacionu jedinicu Policije ili je privremeno udaljen iz službe, neposredni rukovodilac odgovoran je da osigura da su njegova ovlaštenja u informatičkom sistemu ažurirana.

Član 42 (Dostava elektroničkom poštom)

- 1) Elektroničkom poštom dozvoljeno je dostavljati tajne podatke ukoliko je poruka šifrirana korištenjem odobrenih kriptografskih algoritama i ukoliko primalac ima odgovarajuću opremu da obrađuje tajne podatke po odredbama ovog pravilnika.

- 2) Poruke stepena klasifikacije POVJERLJIVO i iznad, koje se prenose elektroničkim

putem trebaju se šifrirati. Poruke stepena klasifikacije INTERNO potrebno je šifrirati prilikom njihovog prenošenja izvan organizacione jedinice pošiljaoca.

3) Porukama je potrebno pružiti istu vrstu zaštite kakva je propisana i za dokumente istog stepena tajnosti. Manipuliranje porukama stepena tajnosti VRLO TAJNO (ukoliko Policija raspolaže sa istima) u centrima veze potrebno je ograničiti na posebno imenovane veziste čiji broj treba održavati na minimumu.

Član 43 (Telekomunikacijsko poslovanje)

Svi tajni podaci prilikom prijenosa moraju biti šifrirani koristeći odobreni kriptografski standard.

Član 44 (Upotreba modema)

1) Nije dozvoljeno postavljanje i upotreba modemskih uređaja na računarima koji se koriste za obradu tajnih podataka.

2) Upotreba modemskog uređaja za potrebe udaljenog nadzora ili upravljanja komunikacijskom ili nekom drugom opremom dozvoljena je samo uz obavezno kriptološko osiguranje i dvostruku autentifikaciju takvih veza kako bi se onemogućila zloupotreba modemskih ulaza.

Član 45 (Upotreba telefaksa)

Telefaks uređajima nije dozvoljeno slanje tajnih podataka bilo koje oznake stepena tajnosti, ukoliko nije zaštićen kriptološki opremom za odgovarajući stepen tajnosti.

Član 46 (Upotreba telefona)

1) Tokom telefonskog razgovora zabranjeno je razmjenjivati tajne podatke sa sagovornikom, ukoliko govorna komunikacija nije zaštićena kriptološko-sigurnosnim sistemom. Za potrebe kriptološki osigurane govorne komunikacije koriste se posebno sigurnosno pripremljeni telefoni u okviru postojeće telefonske mreže. Nezaštićeni prenosivi telefonski aparati neće se koristiti za razgovore o bilo kakvim povjerljivim ili osjetljivim podacima.

2) Ukoliko se telefonskim razgovorom razmjenjuju tajni podaci zabranjeno je uključivanje razglasa na telefonu.

3) Zabranjeno je na uređajima za automatsko primanje govornih poruka ostavljati govorne poruke koje sadrže tajne podatke.

4) Svi nezaštićeni sistemi za prenos podataka, uključujući nezaštićene telefonske aparate, bit će jasno označeni sa oznakom "ZABRANJEN PRENOS TAJNIH PODATAKA".

Član 47

(Videonadzor)

Sve prostorije sigurnosnog područja I i II stepena, uključujući i pomoćne prostorije, sigurnosnu tačku i put do nje, moraju biti pod nadzorom videosistema.

Član 48 (Pregledi protiv prisluškivanja)

1) U svim prostorijama sigurnosnog područja I i II stepena mora biti obavljen pregled protiv prisluškivanja:

- a) kod određivanja sigurnosnog područja,
- b) kod svakog upada u područje,
- c) kod promjene zaposlenih u području i
- d) svakih šest mjeseci.

2) Protivprisluškujuća zaštita drugih sigurnosnih područja ili informacijskih i telekomunikacijskih veza putem kojih se proneše tajni podaci je potrebna ako to zahtijeva ocjena ugroženosti.

3) Protivprisluškujući pregled sigurnosnih područja iz stava 1 ovog člana u Policiji izvodi stručna služba.

Član 49 (Ormari i kase)

1) Tajni podaci stepena tajnosti INTERNO pohranjuju se u uredskim ili metalnim ormarima.

2) Tajni podaci stepena tajnosti POVJERLJIVO pohranjuju se u vatrootpornim ormarima odgovarajućeg stepena čvrstoće.

3) Tajni podaci stepena povjerljivosti TAJNO pohranjuje se u vatrootporne kase sa ugrađenom elektroničkom bravom i neuništivim sistemom javljanja.

4) Tajni podaci stepena tajnosti VRLO TAJNO (ukoliko Policija raspolaže sa istima) pohranjuje se u vatrootpornoj kasi iz stava 3 ovog člana sa dodatno ugrađenim osjetljivim senzorima.

5) U gornjem lijevom kutu vanjske strane ormara odnosno kase iz stavova 1, 2, 3 i 4 ovog člana, treba biti nalijepljena etiketa odgovarajuće veličine sa velikim štampanim slovom:

- a) I za stepen tajnosti INTERNO,
- b) P za stepen tajnosti POVJERLJIVO,
- c) T za stepen tajnosti TAJNO i
- d) VT za stepen tajnosti VRLO TAJNO.

6) Ako se u sigurnosnim ormarima čuvaju podaci različitog stepena tajnosti, vrsta blagajne mora odgovarati najvišem stepenu tajnosti podataka koji se čuvaju u njoj i sa takvim stepenom tajnosti se i označiti.

Član 50

(Kombinacije i ključevi)

- 1) Pojedinačno postavljanje kombinacije elektroničkih i mehaničkih brava na kasama može, zbog obavljanja radnih zadataka u Policiji, poznavati samo osoba koju odredi šef, odnosno zamjenik šefa Policije, i koji moraju radne zadatke u Policiji rasporediti tako da je broj zaposlenika upoznatih sa pojedinim kombinacijama što manji.
- 2) Postavljene kombinacije elektroničkih i mehaničkih brava se mijenjaju:
 - a) odmah nakon postavljanja,
 - b) u slučaju otkrivanja ili sumnje u otkrivanje,
 - c) nakon šest mjeseci od zadnjeg postavljanja zaposlenika,
 - d) kada zaposlenik iz stava 1 ovog člana prestaje obavljati zadatke u Policiji zbog kojih je bio upoznat sa postavljenim kombinacijama i
 - e) kada tako odluči šef Policije, odnosno zamjenik šefa Policije.
- 3) Pismeni zapis pojedinačne kombinacije pohranjuje se u odvojenoj neprovidnoj koverti u kasi jednakog stepena čvrstine kod osobe koju ovlasti šef Policije, odnosno zamjenik šefa Policije.
- 4) Sigurnosni ključevi izdavati će se na revers i to isključivo ovlaštenim licima.
- 5) Vodi se evidencija o svim ključevima, uključujući rezervne ključeve, zajedno sa zapisnikom o pripadajućim bravama ili serijskim brojevima kontejnera / spremnika. Ključevi sigurnosnog područja, odnosno ključevi prostorija iz sigurnosnog područja, pohranjuju se u posebnom prostoru izvan toga područja tako da je neovlaštenim licima pristup onemogućen. Rezervni ključevi stavljaju se u zapečaćene koverta označene sa odgovarajućom sigurnosnom klasifikacijom, a koje se u organizacionoj jedinici drže na sigurnom mjestu u kasi.

Odjeljak C: Organizacione mjere zaštite

Član 51

(Zabranu umnožavanja, kopiranja i prepisivanja)

- 1) Tajni podaci ne smiju se umnožavati, kopirati ili prepisivati, osim ako to nije određeno ovim pravilnikom.
- 2) Tajni podatak stepena tajnosti TAJNO i VRLO TAJNO (ukoliko Policija raspolaže sa istim) ne smije se umnožavati, kopirati ili prepisivati.
- 3) Dodatne primjerke iz stava 2 ovog člana, može izraditi samo ovlaštena osoba koja je odredila stepen tajnosti.
- 4) Izuzetno, ako se radi o tajnim podacima nastalim prije stupanja na snagu Zakona i ovog pravilnika i ako postoji opravdan zahtjev, oni se mogu umnožavati, kopirati ili prepisivati uz prethodnu saglasnost ovlaštene osobe.
- 5) Oprema za umnožavanje postavlja se na mjestima čija je upotreba pod nadzorom ovlaštenih osoba.

Član 52

(Dopušteni izuzeci)

- 1) Izuzetno, može se umnožiti, kopirati ili prepisati zapis ili dio zapisa tajnog podatka stepena tajnosti INTERNO i POVJERLJIVO, ako su ispunjeni slijedeći uslovi:
 - a) pismeno obrazložen zahtjev za umnožavanje, kopiranje ili prepisivanje tajnog podatka sa prijedlogom broja kopija,
 - b) umnožavanje, kopiranje ili prepisivanje tajnog podatka pismeno odobri ovlaštena osoba koja je odredila stepen tajnosti i odredi broj kopija koje će se umnožiti i
 - c) organizaciona jedinica Policije zapis tajnog podatka umnožava u sigurnosnom području odgovarajućeg stepena.
- 2) O umnožavanju dokumenata ili medija koji su označeni stepenom tajnosti INTERNO ili POVJERLJIVO vodi se evidencija o umnožavanju.
- 3) U evidenciju iz stava 2 ovog člana upisuju se slijedeći podaci:
 - a) broj i oznaka stepena tajnosti,
 - b) datum, vrijeme i mjesto umnožavanja,
 - c) ime i prezime zaposlenika koji je obavio umnožavanje,
 - d) osnov umnožavanja (zahtjev i odobrenje),
 - e) broj izrađenih fotokopija i
 - f) nazivi primaoca svake pojedine fotokopije.

Član 53 (Uništavanje dokumenata)

- 1) Tajni podaci se moraju uništiti na način da se tajni podatak ne može raspoznati i obnoviti.
- 2) Šef Policije će odrediti komisiju za uništavanje dokumenata ili medija iz stava 1 ovog člana koja sačinjava zapisnik o uništavanju. Komisiju čine tri policijska službenika. Članovi komisije moraju imati dozvolu za pristup tajnim podacima.
- 3) Komisija će, nakon što sačini zapisnik, dostaviti ga šefu Policije na verifikaciju.
- 4) Šef Policije će, na prijedlog zamjenika šefa Policije, donijeti plan uništavanja tajnih podataka u vanrednim okolnostima.
- 5) O uništavanju tajnih podataka stepena tajnosti VRLO TAJNO (ukoliko Policija raspolaže sa istima) pismeno se obavještava organ koji je odredio taj stepen tajnosti.

Član 54 (Prenošenje ili slanje tajnih podataka)

- 1) Tajni podaci se prenose u zatvorenoj, neprovidnoj koverti.
- 2) Tajni podaci stepena tajnosti INTERNO mogu se prenositi vlastitom prijenosnom mrežom ili preporučenom poštom s povratnicom, a tajni podaci stepena tajnosti POVJERLJIVO ili višeg stepena tajnosti mogu se prenositi vlastitom prijenosnom mrežom ili kurirskom službom.
- 3) Tajni podatak stepena tajnosti POVJERLJIVO ili višeg stepena tajnosti prenose se u

dvije koverta. Vanjska koverta je od tvrdog neprovidnog, nepropusnog materijala. Na njoj moraju biti podaci o primaocu, pošiljaocu i šifra dokumenata. Iz oznaka na vanjskoj koverti ne smije se vidjeti da se radi o tajnom podatku. Unutrašnja koverta mora imati oznaku stepena tajnosti, šifru dokumenata, podatke o primaocu i pošiljaocu i druge podatke koji su važni za tajnost.

4) Pri prenošenju tajnih podataka stepena tajnosti POVJERLJIVO ili TAJNO izvan sigurnosnog područja, vanjsku omotnicu može zamijeniti zatvoren ili zapečaćen kofer, kutija ili torba.

5) Pri prenošenju tajnih podataka stepena tajnosti VRLO TAJNO (ukoliko Policija raspolaže sa istima) izvan sigurnosnog područja, unutrašnja omotnica mora biti u zatvorenom koferu, kutiji ili torbi sa zatvaranjem na ključ ili sa šifriranom kombinacijom. Prijenos moraju obavljati najmanje dvije osobe.

6) Kada se tajni podaci iz stavova 4 i 5 ovog člana prenose unutar sigurnosnog ili administrativnog područja, prenose se tako da se onemogućí opažanje njihovog sadržaja.

7) Policija mora odrediti gdje se primaju nosioci tajnih podataka i ko ih prima. Primalac ili osoba koja je ovlaštena za prijem nosilaca tajnih podataka potvrđuje njihov prijem upisom u dostavnu, odnosno kurirsku knjigu.

8) Kuriri i druge osobe, koji prenose tajne podatke moraju biti sigurnosno provjereni u odnosu na stepen tajnosti tajnih podataka koje prenose.

Član 55 (Kurirska služba)

1) Policija za prijenos tajnih podataka stepena tajnosti TAJNO ili višeg stepena izvan sigurnosnog područja izrađuje nacrt puta i sigurnog prijenosa tajnih podataka.

2) Nacrti osiguranja prijenosa tajnih podataka stepena tajnosti TAJNO ili višeg stepena moraju sadržavati postupke i mjere pri mogućem pokušaju oduzimanja, oštećenja ili uništenja, saobraćajnih i drugih događaja. U nacrtu moraju biti određeni glavni i sporedni putevi.

3) Kuriri koji prenose tajne podatke stepena tajnosti TAJNO ili višeg stepena moraju biti osposobljeni i upoznati sa postupcima i mjerama pri zaštiti tajnih podataka. Kuriri trebaju proći sigurnosnu provjeru za pristup tajnim podacima najmanje onog stepena tajnosti koji ima dokument koji će se prenositi.

Član 56 (Ovlaštenje za prenos)

1) Kuriri koji prenose tajne podatke stepena POVJERLJIVO ili višeg stepena moraju imati pismeno ovlaštenje šefa Policije za prijenos tajnih podataka i moraju ga pokazati na zahtjev osobe kojoj poštu predaje ili od koje je preuzima.

2) Sadržaj i oblik ovlaštenja dati su na obrascu broj 5 koji je sastavni dio ovog pravilnika.

Član 57 (Evidencije)

- 1) Evidencija tajnih podataka se vodi odvojeno od ostalih evidencija.
- 2) U dokumentu koji sadrži tajne podatke se, ispred broja predmeta, označi stepen tajnosti podataka i to velikim štampanim slovom:
 - a) I - za stepen tajnosti INTERNO,
 - b) P - za stepen tajnosti POVJERLJIVO,
 - c) T - za stepen tajnosti TAJNO i
 - d) VT - za stepen tajnosti VRLO TAJNO.
- 3) Evidencija iz stava 1 ovog člana sadrži sljedeće rubrike: redni broj, naziv Policija Brčko distrikta BiH - naziv organizacione jedinice koja je odredila stepen tajnosti, predmet podneska, datum prijema podneska, klasifikaciona oznaka, organizaciona jedinica koja rukuje tajnim podatkom, ustupljeno drugom organu - datum, promjena stepena tajnosti - datum, prestanak tajnosti - datum, rješenje - datum, arhiva -datum, napomena.
- 4) Izgled evidencije iz stavova 1 i 3 ovog člana dat je na obrascu broj 6 koji je sastavni dio ovog pravilnika.

Član 58 (Omot za predmete i akte)

- 1) Prednja strana omota za predmete i akte koji sadrže tajne podatke ima odgovarajuću boju širine 3 cm, mjereno od vanjskih ivica prema unutrašnjosti omota i to:
 - a) stepen tajnosti VRLO TAJNO - crvena,
 - b) stepen tajnosti TAJNO - žuta,
 - c) stepen tajnosti POVJERLJIVO - plava i
 - d) stepen tajnosti INTERNO - siva.
- 2) Omot iz stava 1 ovog člana izrađuje se prema obrascu broj 7 koji je sastavni dio ovog pravilnika.

Član 59 (Spisak uvida)

- 1) Policija kada pohranjuje tajne podatke označene stepenom T AJNO ili VRLO T AJNO (ukoliko Policija raspolaže sa istima) vodi spisak uvida u kojem se evidentiraju sljedeći podaci:
 - a) kratak sadržaj predmeta, broj, datum, stepen tajnosti i broj primjeraka dokumenta koji sadrži tajni podatak,
 - b) ime i prezime osobe koja se upoznala sa tajnim podatkom,
 - c) razlog upoznavanja,
 - d) datum i vrijeme upoznavanja i
 - e) potpis osobe koja se upoznala sa tajnim podatkom.
- 2) Spisak uvida nalazi se uz svaki primjerak dokumenta ili medija označenog stepenom TAJNO ili VRLO TAJNO.

Član 60

(Primjena propisa o arhiviranju)

Dokumenti koji sadrže tajne podatke arhiviraju se u skladu s propisima koji uređuju arhivsku djelatnost.

Član 61 (Pohranjivanje arhivskih primjeraka)

1) Arhivski primjerak dokumenta označenog stepenom tajnosti TAJNO ili VRLO TAJNO (ukoliko Policija raspolaže sa istima) je po pravilu primjerak broj 1 ovlaštene osobe Policije koja je odredila stepen tajnosti.

2) Uz arhivski primjerak dokumenta iz stava 1 ovog člana, čuva se i pismena procjena na osnovu koje se podatku određuje stepen tajnosti, spisak organa odnosno osoba, kojima su primjerci tajnih podataka bili uručeni, spisak uvida, te moguće dozvole za umnožavanje tajnog dokumenta.

Član 62 (Plan čuvanja)

Policija će, uz uvažavanje mjera određenih ovim pravilnikom, sačiniti plan čuvanja tajnih podataka kojim detaljnije određuje fizičke, tehničke i organizacione mjere te postupke za čuvanje tajnih podataka s obzirom na stepen tajnosti i procjenu ugroženosti.

Član 63 (Sadržaj plana osiguranja)

1) Plan osiguranja se sastoji od općeg i posebnog dijela.

2) Opći dio sadrži naročito:

- a) procjenu ugroženosti,
- b) opis glavnog i pomoćnih objekta Policije (položaj, ulazi, izlazi, nužni izlazi, skica odnosno fotografije objekta, glavne i rezervne puteve do objekta te podatke o sigurnosnoj i tehničkoj opremi),
- c) podatke o nosiocu sigurnosnog plana,
- d) definiranje sigurnosnih područja i
- e) mjere čuvanja zaposlenika koji se bave tajnim podacima.

3) Posebni dio sadrži naročito:

- a) mjere fizičkog osiguranja (vanjsko i unutrašnje fizičko osiguranje, sigurnosne tačke sa opisom zadataka izvođača),
- b) mjere tehničkog osiguranja (vanjsko i unutrašnje tehničko osiguranje, kontrola ulaza i izlaza, alarmni sistem i postupke pri aktiviranju pojedinih stepena alarma, dokumentiranje) i
- c) postupke za nasilno ulaženje i nepredviđene događaje sa planom uništavanja.

4) Zamjenik šefa Policije je odgovoran za izradu plana osiguranja.

5) Policija može imati i zajednički plan osiguranja za objekat u sjedištu i sve druge objekte Policije.

Član 64

(Provjeravanje efikasnosti plana osiguranja)

- 1) PolICIJA će ažurirati plan osiguranja svakih šest mjeseci i po potrebi ga dopunjavati.
- 2) Plan osiguranja potrebno je najmanje jednom godišnje pregledati, te provjeriti efikasnost mjera koje su njime određene.

Član 65 (Zloupotreba tajnog podatka)

- 1) Sa svakim neovlaštenim pristupom tajnim podacima, njihovim uništenjem, krađom ili drugim događajem koji ukazuje na zloupotrebu tajnih podataka treba odmah upoznati šefa PolICIJE, odnosno zamjenika šefa PolICIJE i osigurati sve mjere za onemogućavanje dalje zloupotrebe tajnog podatka, te provesti istragu o okolnostima zloupotrebe.
- 2) Šef PolICIJE mora o događaju iz stava 1 ovog člana obavijestiti organ koji je odredio tajni podatak.
- 3) O svakoj zloupotrebi tajnog podatka obavijestit će se državni sigurnosni organ.
- 4) PolICIJA će propisati odgovarajuće postupke i mjere vezano za zloupotrebu tajnih podataka.

Član 66 (Obavještenje o zloupotrebi tajnog podatka)

Obavještenje o zloupotrebi tajnog podatka mora sadržavati:

- a) podatke potrebne za identifikaciju tajnog podatka (opis medija koji sadrži tajni podatak uključeno sa stepenom tajnosti podataka, šifru i datum dokumenta, broj kopije vlasnika i kratki sadržaj),
- b) kratak opis okolnosti o zloupotrebi tajnog podatka i ako je poznato broj osoba koje su ili su mogle imati dostup tajnom podatku,
- c) informaciju da li je vlasnik podatka bio obaviješten i
- d) postupke i mjere koji su bili izvedeni da se spriječi daljnja zloupotreba tajnih podataka.

DIO ŠESTI- PRIJELAZNE I ZAVRŠNE ODREDBE

Član 67 (Označavanje tajnih podataka iz člana 86 Zakona)

- 1) Tajnim podacima kojima je oznaka stepena tajnosti određena prije stupanja na snagu Zakona, određuje se novi stepen tajnosti u skladu s članom 86 Zakona.
- 2) Na dokumentima iz stava 1 ovog člana precrtava se stara oznaka stepena tajnosti. Ispod te oznake upisuje se oznaka novog stepena tajnosti, te datum i potpis ovlaštene osobe u PolICIJI koja je tu promjenu učinila.

Član 68 (Obaveze u prethodnom periodu)

- 1) Kabinet šefa PolICIJE, posebno u oblasti telekomunikacija i informacione tehnologije izvršit će potrebne pripreme i predložiti donošenje posebnih instrukcija radi usklađivanja

s odredbama ovog pravilnika u roku od 24 mjeseca od dana stupanja na snagu ovog pravilnika.

2) Kabinet šefa Policije će u roku iz stava 1 ovog člana pripremiti sve potrebne štambilje i izvršiti ostale pripreme u skladu s odredbama ovog pravilnika.

3) Planom kapitalnih ulaganja Policija će blagovremeno osiguravati finansijska sredstva potrebna za realizaciju mjera i zadataka koji proističu iz zakona, podzakonskih akata Vijeća ministara BiH i ovog pravilnika.

Član 69 (Stupanje na snagu)

Ovaj pravilnik stupa na snagu danom donošenja i objavit će se u „Službenom glasniku Brčko distrikta BiH“.

Broj: 14.05/1-02-3190/08
Brčko, 08. 04. 2008. godine

Šef Policije Brčko distrikta BiH
Goran Lujčić, s.r.