PRAVILNIK

O NAČINU I OBLIKU OZNAKA TAJNOSTI PODATAKA, TE FIZIČKIM, ORGANIZACIJSKIM, TEHNIČKIM MJERAMA I POSTUPCIMA ZA ČUVANJE TAJNIH PODATAKA

I - OPĆE ODREDBE

Član 1.

(Predmet Pravilnika)

Ovim Pravilnikom bliže se uređuje način i oblik označavanja tajnih podataka, fizičke, organizacijske, tehničke mjere i postupci za čuvanje tajnih podataka, kojih se moraju pridržavati svi organi iz člana 2. Zakona o zaštiti tajnih podataka (u daljnjem tekstu: Zakon).

Član 2.

(Cilj mjera čuvanja)

(1) Cilj mjera neposrednog fizičkog čuvanja tajnih podataka, osiguravanja prostora i objekata (fizičke mjere), mjera postupanja organa u pripremanju, ustupanju, čuvanju i uništavanju tajnih podataka (organizacijske mjere) te mjera čuvanja tajnih podataka, osiguravanje prostorija ili objekata sa tehničkim sredstvima u skladu sa ovim Pravilnikom (tehničke mjere), je onemogućavanje pristupa odnosno otkrivanja tajnih podataka neovlaštenim licima.

(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.

II - NAČIN I OBLIK OZNAČAVANJA TAJNIH PODATAKA

Član 3.

(Oznaka)

(1) Svaki dokument ili medij koji sadrži tajni podatak mora biti označen:

a) stepenom tajnosti;

b) podacima o organu, organizaciji, ili instituciji čija je ovlaštena osoba odredila tajnost;

c) podacima o ovlaštenom licu (ime i prezime, broj i datum ovlaštenja);

d) datumom određivanja tajnih podataka;

e) načinom prestanka tajnosti u skladu sa odredbama člana 25. Zakona i

f) načinom dostavljanja.

(2) Svaki dokument ili medij koji je označen stepenom tajnosti VRLO TAJNO i TAJNO pored podataka iz stava 1. ovog člana mora imati i podatke o:

a) broju primjerka dokumenta,

b) ukupnom broju stranica dokumenta i

c) mogućim prilozima 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 br. 1. i 2. koji su sastavni dio ovog Pravilnika.

(6) Obrasci broj 1. i 2. nalaze se u omotu spisa i vidljivi su odmah pri otvaranju omota.

Član 4.

(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 pri dnu pored stepena tajnosti naveden i redni broj strane s obzirom na ukupan broj strana dokumenta (npr 4/8). Ako pisani dokument nema naslovnu stranu, prva strana će se smatrati 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 elektronskih zapisa) 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, isti 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 sa stepenom tajnosti ima dodatne dijelove (npr. aneksi, dodaci, grafički prikazi i sl) isti će se označiti 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 vrši dostavljanje tajnih podataka označavaju se istim stepenom tajnosti kao i dokument koji se dostavlja.

Član 5.

(Dodatne oznake)

Svaki dokument ili medij, koji je označen stepenom tajnosti VRLO TAJNO, dodatno se označava crnom linijom debljine najmanje četiri milimetra, kojom se podvlači samo stepen tajnosti.

Član 6.

(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 kraju svakog pasusa upišu oznake (I) (P) (T) (VT);

b) je dokumenat, koji sadrži više pasusa različitog stepena tajnosti označen sa najvišim stepenom tajnosti pojedinačnog pasusa;

c) se u prostor za dodatne oznake upiše "Pasusi su označeni sa različitim stepenom tajnosti".

(2) Ovlašteno lice koje je odredilo stepen tajnosti mora u pismenoj ocjeni zapisati i razloge za određivanje različitog stepena tajnosti pojedinačnih pasusa.

Član 7.

(Označavanje dodatnih kopija)

(1) Svaka dodatna kopija dokumenta ili medija ili njihovog dijela mora biti označena na način propisan u čl. 3 i 4. ovog Pravilnika.

(2) Kopija iz stava 1. ovog člana, dodatno se označava: oznakom "kopija orginala", rednim brojem kopije, brojem i datumom iz evidencije o umnožavanju, oznaka organizacione jedinice i potpis službenika koji je izvršio umnožavanje.

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

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

Član 8.

(Oznaka promjene stepena tajnosti)

(1) Ukoliko ovlašteno lice donese odluku o promjeni stepena tajnosti dokumenta ili medija, o istom 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 sljedeće:

a) prekrižiti originalnu oznaku;

b) dokument ili medij označiti na posebnom listu sa odgovarajućom oznakom iz člana 3. ovog Pravilnika, koja uključuje i navođenje broja i datuma pismene obavijesti o promjeni stepena tajnosti;

c) datum i potpis ovlaštenog lica organa koji je oznaku prepravio.

(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 isti se označava na način da se prekriži oznaka stepena tajnosti i ispod toga upiše "PRESTANAK TAJNOSTI", datum prestanka i potpis ovlaštene osobe.

Član 9.

(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.

III. FIZIČKE MJERE ZAŠTITE

Član 10.

(Opće)

(1) Svi objekti, zgrade, uredi, sobe i drugi prostori gdje se arhiviraju tajni podaci i gdje se njima rukuje, trebaju biti zaštićeni odgovarajućim mjerama fizičke zaštite. Kod odlučivanja o stepenu potrebne fizičke sigurnosne zaštite, u obzir će se uzeti relevantni faktori kao što su:

(a) nivo povjerljivosti i kategorija informacije;

(b) količina i oblik informacija (štampane na papiru/ na medijima za kompjutersko pohranjivanje);

(c) sigurnosna provjera i osoblje koje treba znati informacije;

(d) kako će se arhivirati informacije.

(2) Mjere fizičke sigurnosti će biti tako osmišljene da:

a) spriječe nedozvoljen ili nasilan upad od strane neovlaštene osobe;

b) odvrate, spriječe i otkriju radnje neovlaštene osobe;

c) omoguće selekciju osoblja u pogledu pristupa tajnim podacima i

d) omoguće otkrivanje i postupanje u svim slučajevima ugrožavanja sigurnosti što je prije moguće.

Član 11.

(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, elektronskih 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 elektronskim sistemom za protivprovalno osiguranje sigurnosnog područja, čiji je alarmni sistem povezan sa jedinicom odgovornom za intervenciju prilikom alarma (nadzorni 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 nadzornog centra i sistem mora imati osigurano rezervno napajanje,

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, koja 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, koji osigurava, da druge osobe ulaze u sigurnosno područje samo u pratnji zaposlene osobe ili uz izvođenje odgovarajućeg oblika nadzora, koji osigurava, da će osoba ulaziti samo u dijelove područja, povezane sa razlogom ulaska i ako je to potrebno upoznat će se 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, elektronskih i magnetno-optičkih sastavnih dijelova, kojima bi bilo moguće tajne podatke neovlašteno snimiti, odnijeti ili prenijeti, je dozovljen, ali sva oprema mora biti isključena. Svaku njenu upotrebu odobrava osoba odgovorna za sigurnost područja;

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, se uspostavlja administrativno područje, koje može zahvatati sve službene prostorije organa. Za takvo područje određuje se lokacija na kojoj organ može nadzirati ulaženje 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 od strane rukovodioca organa u kojoj je sigurnosno područje, odnosno osobe koju je rukovodilac organa pismeno ovlastio.

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

Član 12.

(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.). Organ 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) O izgledu sigurnosne propusnice i njihovoj tehničkoj izradi odlučuje rukovodilac organa.

Član 13.

(Određivanje sigurnosnog i administrativnog područja)

(1) Određivanje stepena klasifikacije sigurnosnih i administrativnih područja i stepena njihove zaštite odgovarat će značaju podataka sa sigurnosnog aspekta koje je potrebno zaštititi.

(2) Rukovodilac organa odlukom određuje sigurnosna i administrativna područja uz prethodno pribavljeno mišljenje državnog sigurnosnog organa o odgovarajućoj sigunosno-tehničkoj opremi ugrađenoj u sigurnosno područje, kao i postupke i mjere osiguranja sigurnosnog područja.

Član 14.

(Označavanje sigurnosnih i administrativnih područja)

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

(2) Obavještenje iz stava 1. ovog člana mora sadržavati vidne natpise: "naziv organa-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 1. ovog člana, ali to područje odnosno zgrada ili okoliš u kojem je područje, mora biti označeno tablama na kojima je napisano ime organa te obavještenje o nadzoru pristupa i kretanja, ako se ono izvodi.

(4) Izuzetno, kad to zahtijevaju posebne okolnosti, rukovodilac organa 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 organa.

Član 15.

(Nadzor ulaza i izlaza)

(1) Ulazak stalno zaposlenog osoblja u sigurnosna i administrativna područja nadzire se utvrđivanjem identiteta osoba koje ulaze. Fizički nadzor ulaska može dopunjavati sistem

automatskog prepoznavanja identifikacijskih kartica odnosno biometrijskih oznaka osoba koje ulaze.

(2) Prije ulaska drugih osoba u sigurnosno i administrativno područje, osoba koja nadzire ulazak u sigurnosno područje, mora provjeriti njihov identitet i razlog ulaska, kao i ispunjavanje drugih uvjeta 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 st. 2 i 3. ovog ovog člana upisuju se u evidenciju ulaska i kretanja u sigurnosnom području organa.

(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 promjenjene sigurnosne prilike.

(6) U prostore koji su posebno namjenjeni za rad sa strankama, mogu posjetioci i druge osobe u pratnji stranke ulaziti i izlaziti u prisustvu zaposlenih osoba u organu 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 16.

(Osiguranje opreme)

(1) Fotokopirni strojevi, telefaksi i druge naprave za obradu tajnih podataka, koji su postavljeni u sigurnosnom području moraju biti osigurani tako da ih mogu upotrebljavati osobe koje su ovlaštene za rad sa tim aparatima.

(2) Sva elektronska 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 17.

(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. Osoba koja 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 određenog organa, odgovorna osoba 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. Osoba koja preuzme tajni podatak, potvrđuje to sa vlastoručnim potpisom i s tim preuzima brigu za sigurnost tajnog podatka.

IV - TEHNIČKE MJERE ZAŠTITE

Član 18.

(Opće)

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

Član 19.

(Izgradnja objekata)

(1) Kod izgradnje i uređenja objekata mora se voditi računa da prostori u kojem 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 onemogućuju pogled u unutrašnjost prostorije te sa sigurnosnim zvučno izoliranim ulaznim vratima s mehanizmom za samozatvaranje, bez ostakljenja iznad vrata.

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

(3) Ako je prostor iz stava 1. ovog člana u potkrovlju građevine onda ne smije imati krovne prozore.

Član 20.

(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 zatamnjenim staklima koja onemogućavaju pogled u unutrašnjost prostorije.

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

(3) Ukoliko građevinski objekt nema iskoristiv prostor u prizemlju izuzetno se može koristiti i prostor na višim spratovima ispunjavajući sve uvjete 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 21.

(Prostorije za smještaj sigurnosne opreme)

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

a) jednim od pristupnih sigurnosno-zaštitnih mehanizama na ulaznim vratima, s mogućnošću arhiviranja podataka o ulasku u prostor (pristupni štampač, biometrični sistem itd.) kako bi se pristup takvim prostorijama mogao ograničiti i nadzirati;

b) opremom za sigurno arhiviranje i čuvanje predmeta i dokumenata;

c) energetskim priključkom na centralno neprekidno i agregatsko napajanje;

d) sigurnosnim mehaničkim sistemom za zaključavanje s ograničenim brojem ključeva bez mogućnosti umnožavanja ili tome odgovarajuća odvojena automatizirana i manualna rješenja.

Član 22.

(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 strane tog korisnika na računar posebne namjene (Log. Server);

b) modul za onemogućavanje neovlaštenog kopiranja podataka sa i na prijenosne magnetne 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, flopy, traka…) i optičkim (CD, DVD…) medijima u slučaju da su isti neovlašteno korišteni.

Član 23.

(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 odgovornih za sigurnost informacija pohranjenih na datim računarima;

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 TAJNA 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 odredio lokalni organ za sigurnost.

(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 24.

(Preduvjeti za korištenje računarske opreme)

(1) Samo odobreni hardveri će se koristiti ili priključivati na informacijsko-komunikacijski sistem. Bez prethodnog odobrenja nadležnog organa za sigurnost, 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 TAJNA i iznad potrebno je evidentirati, zaštititi i pregledati na sličan način kao i papirnu dokumentaciju istog stepena klasifikacije. Za fiksne hard drajvove stepena klasifikacije TAJNA ili iznad, 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 softwerski moduli moraju biti provjereni da ne sadrže dokumentovane ili nedokumentovane procedure ili funkcije koje mogu smanjiti sigurnost sistema.

Član 25.

(Informatičko osoblje)

(1) Svaki sistem informatičke tehnologije (informacijsko-komunikacijski sistem) posluživat će osoblje za osiguranje odgovarajuće strukture za upravljanje sigurnosnim mjerama radi sprovođenja

i održavanja mjera zaštite informacijsko-komunikacijskog sistema koje će se primjenjivati na datoj lokaciji. Osoblje za osiguranje informacijsko-komunikacijskog sistema bit će uključeno u organizaciju za upravljanje sigurnosnim mjerama. Za veći informacijsko-komunikacijski sistem ili specifična područja (naprimjer, odjeljenja ili direkcije jedne organizacije), imenovat će se dodatno osoblje 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/njenom 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 osoblju 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 26.

(Obaveze u radu s informatičkom opremom)

(1) Organ za sigurnost informacijsko-komunikacijskog sistema formulirat će politiku za ograničavanje broja aktivnih pomoćnih drajvova i uređaja u područjima odgovornosti. Prilikom formuliranja ovih sigurnosnih politika, primjenit će se sljedeći uvjeti:

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 odsjeku ili odjelu. Gdje god je to moguće, ovi aktivirani drajvovi nalazit će se u administrativnom odjeljenju odsjeka/odjela;

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 organizacije/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 potrebno 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 "Strogo Povjerljivo" ili onima posebne vrste. Svi pojedinci koji imaju operativnu potrebu da koriste uređaje USB za pohranjivanje velike količine podataka na povjerljivom informacijsko-komunikacijskom sistemu ili informacijsko-komunikacijskom sistemu za povjerljive misije morat će podnijeti zahtjev nadležnom organu za sigurnost navodeći operativnu potrebu. Lokalni sigurnosni ili izvršni organi vršit će potvrdu valjanosti svih zahtjeva za korišćenje uređaja USB na informacijsko-komunikacijskim sistemima BEZ SIGURNOSNE KLASIFIKACIJE. Svi uređaji USB za pohranjivanje velike količine podataka trebaju se označiti i manipulirati u skladu sa najvećim stepenom tajnosti podataka koji su ikad bili sadržani na ovom uređaju ili najvećim stepenom klasifikacije 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 prijaviti. Za informacijsko-komunikacijske sisteme stepena klasifikacije TAJNA, samo oni terminali koji se nalaze u području koje je pod nadzorom (kao što je Registar, područja sa ljudskom posadom/stražom 24 sata 7 dana u sedmici) treba da imaju mogućnost korištenja uređaja USB za pohranjivanje velike količine podataka;

e) priključivanje digitalnih kamera na informacijsko-komunikacijske sisteme s 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 osoblje koje je odgovorno za uploading (prijenos podataka sa računara na server)/ 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, te koje je odobrio nadležni organ za sigurnost. 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. Bez odobrenja nadležnog organa za sigurnost neće se vršiti nikakve izmjene konfiguracije softvera ili samog softvera, a bez prethodnog odobrenja ograna za sigurnost neće se vršiti nikakve softverske izmjene koje bi utjecale na sigurnosni profil jednog sistema;

g) ovlašteni korisnici informacijsko-komunikacijskog sistema neće dozvoliti nikome drugom, uključujući 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 koje se nalaze na računarima pod njegovom administrativnom kontrolom.

(3) Svaki informacijski sistem mora imati servere u mrežnom opertivnom 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.

(4) 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 će da 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/opreme.

Član 27.

(Obaveze korisnika)

(1) Svaki korisnik je pojedinačno 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;

c) prijavi svaki sigurnosni incident ili neobičan događaj koji se može opaziti tokom rada informacijsko-komunikacijskog sistema.

(2) Službenici 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;

c) aktivirati sigurnosno-zaštitne mehanizme računarske jedinice od mogućeg djelovanja računarskih virusa prilikom predaje ili prijema bilo kojeg spisa.

Član 28.

(Obaveze kod promjene radnog statusa)

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

Član 29.

(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 elektronskim putem trebaju se šifrirati. Poruke stepena klasifikacije INTERNO potrebno je šifrirati prilikom njihovog prenošenja izvan organizacije pošiljaoca.

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

Član 30.

(Telekomunikacijsko poslovanje)

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

Član 31.

(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 authentikaciju takvih veza kako bi se onemogućila zlopotreba modemskih ulaza.

Član 32.

(Upotreba telefaxa)

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

Član 33.

(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 prijenos podataka, uključujući nezaštićene telefonske aparate, bit će jasno označeni sa oznakom: "ZABRANJEN PRENOS TAJNIH PODATAKA".

Član 34.

(Video nadzor)

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

Član 35.

(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) Protiv prisluškujuća zaštita drugih sigurnosnih područja ili informacijskih i telekomunikacijskih veza putem kojih se prenose tajni podaci je potrebna ako to zahtijeva ocjena ugroženosti.

(3) Protiv prisluškujući pregled sigurnosnih područja iz stava 1. ovog člana u ministarstvu odbrane i drugim organima i organizacijama iz oblasti sigurnosti izvode stručne službe tih organa.

(4) U drugim organima i organizacijama protiv prisluškujući pregled sigurnosnih područja iz stava 1. ovog člana obavlja stručna služba policijskog organa.

Član 36.

(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 pohranjuju se u vatrootporne kase sa ugrađenom elektronskom bravom i neuništivim sistemom javljanja.

(4) Tajni podaci stepena tajnosti VRLO TAJNO pohranjuju se u vatrootpornoj kasi iz prošlog stava sa dodatno ugrađenim osjetljivim senzorima.

(5) U gornjem lijevom kutu vanjske strane ormara odnosno kase iz prethodnih stavova ovog člana nalijepi se 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;

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 37.

(Kombinacije i ključevi)

(1) Pojedinačno postavljanje kombinacije elektronskih i mehaničkih brava na kasama može zbog obavljanja radnih zadataka u organu poznavati samo osoba koju odredi rukovodilac organa. Rukovodilac organa mora radne zadatke u organu rasporediti tako da je broj osoba upoznatih sa pojedinim kombinacijama što manji.

(2) Postavljene kombinacije elektronskih i mehaničkih brava se mijenjaju:

a) odmah nakon postavljanja;

b) u slučaju otkrivanja ili sumnje u otkrivanje;

c) nakon šest mjeseci od zadnjeg postavljanja službenika;

d) nakon toga kada osoba iz prošlog stava prestaje obavljati zadatke u organu zbog kojih je bila upoznata sa postavljenim kombinacijama i

e) kada tako odluči rukovodilac organa.

(3) Pismeni zapis pojedinačne kombinacije pohranjuje se u odvojenoj neprovidnoj koverti u kasi jednakog stepena čvrstine kod rukovodioca organa, odnosno kod osobe koju je on ovlastio.

(4) Sigurnosni ključevi izdavat će se na revers i to isključivo ovlaštenim licima.

(5) Održavat će 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 stavljat će se u zapečaćene koverte označene sa odgovarajućom sigurnosnom klasifikacijom, a koje će nadležni organ držati na sigurnosnom mjestu u kasi.

V - ORGANIZACIONE MJERE ZAŠTITE

Član 38.

(Zabrana 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 ne smije se umnožavati, kopirati ili prepisivati.

(3) Dodatne primjerke iz stava 2. ovog člana, može izraditi samo ovlašteno lice koje je odredilo stepen tajnosti.

(4) Izuzetno, ako se radi o tajnim podacima nastalim prije stupanja na snagu zakona i ovog Pravilnika i ako postoji opravdan zahtjev, isti se mogu umnožavati, kopirati ili prepisivati uz prethodnu saglasnost ovlaštenog lica.

(5) Oprema za umnožavanje postavlja se na mjestima čija je upotreba pod nadzorom ovlaštenih osoba.

Član 39.

(Dopušteni izuzeci)

(1) Izuzetno, može se umnožiti, kopirati ili prepisati zapis ili dio zapisa tajnog podatka stepena tajnosti INTERNO i POVJERLJIVO ako su ispunjena tri uvjeta:

a) pismeno obrazložen zahtjev za umnožavanje kopiranje ili prepisivanje tajnog podatka sa prijedlogom broja kopija;

b) umnožavanje, kopiranje ili prepisivanje tajnog podatka pismeno odobri ovlašteno lice koje je odredilo stepen tajnosti i odredi broj kopija koje će se umnožiti;

c) organ ili organizacija 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 službenika koji je obavio umnožavanje;

d) osnov umnožavanja (zahtjev i odobrenje);

e) broj izrađenih fotokopija;

f) nazivi primaoca svake pojedine fotokopije.

Član 40.

(Uništavanje dokumenata)

(1) Tajni podaci se moraju uništiti na način da se tajni podatak ne može raspoznati i obnoviti.

(2) Rukovodilac organa odredit će komisiju za uništavanje dokumenata ili medija iz stava 1. ovog člana koja sačinjava zapisnik o uništavanju. Članovi komisije moraju imati dozvolu za pristup tajnim podacima.

(3) Komisija će nakon što sačini zapisnik isti dostaviti rukovodiocu organa na verifikaciju.

(4) Rukovodilac organa dužan je sačiniti plan uništavanja tajnih podataka u vanrednim okolnostima.

(5) O uništavanju tajnih podataka stepena tajnosti VRLO TAJNO pismeno se obavještava organ koji je odredio taj stepen tajnosti.

Član 41.

(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 putem preporučene pošte s povratnicom, tajni podaci stepena tajnosti POVJERLJIVO ili višeg stepena tajnosti putem vlastite prijenosne mreže ili putem kurirske službe (u daljnjem tekstu: kurirska služba)

(3) Tajni podatak stepena tajnosti POVJERLJIVO i višeg stepena tajnosti prenose se u dvije koverte. Vanjska koverta je od tvrdog, neprovidnog, nepropusnog materijala. Na njoj moraju biti podaci o primaocu, pošiljaocu i šifra dokumenta. Iz oznaka na vanjskoj koverti ne smije se vidjeti da se radi o tajnom podatku. Unutrašnja koverta mora imati oznaku stepena tajnosti, šifru dokumenta, 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 zapečačen kofer, kutija ili torba.

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

(6) Kada se tajni podaci iz st. 4 i 5. ovog člana prenose unutar sigurnosnog ili administrativnog područja, moraju biti sakriveni tako da se onemogući opažanje njihovog sadržaja.

(7) Svaki organ 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 (u daljnjem tekstu: kuriri) moraju biti sigurnosno provjereni u odnosu na stepen tajnosti tajnih podataka koje prenose.

Član 42.

(Kurirska služba)

(1) Organi moraju za prijenos tajnih podataka stepena tajnosti TAJNO ili višeg stepena izvan sigurnosnog područja izraditi 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 ili drugih nesreća, zastoja, kratkog stajanja, noćenja 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 kod zaštite tajnih podataka. Kuriri trebaju proći sigurnosnu provjeru za pristup tajnim podacima najmanje onog stepena tajnosti koji ima dokument koji će se prenositi.

(4) Kuriri, koji prenose tajne podatke osposobljavaju se najmanje jedanput godišnje, a osposobljavanje vrši državni sigurnosni organ.

Član 43.

(Ovlaštenje za prijenos)

(1) Kuriri, koji prenose tajne podatke stepena POVJERLJIVO ili višeg stepena, moraju imati pismeno ovlaštenje rukovodioca organa 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 44.

(Pomoć drugih organa)

(1) Po potrebi, nadležni policijski organ pruža kuriru koji prenosi tajne podatke pomoć u obliku i obimu, koji omogućava osiguranje tajnih podataka od otuđenja, oštećenja i uništenja.

(2) Ovlaštene osobe nadležnog policijskog organa iz stava 1. ovog člana nemaju prava uvida u sadržinu tajnih podataka.

(3) Službenici carinske službe kod postupaka koji izvode u skladu sa svojim ovlaštenjima, nemaju pravo uvida u sadržinu tajnih podataka, kada kurir predoči važeće ovlaštenje.

Član 45.

(Međunarodna razmjena tajnih podataka)

(1) Međunarodno razmjenjivi podaci su tajni podaci koji se na osnovu međunarodnog ugovora dostavljaju međunarodnoj organizaciji, drugoj državi odnosno državnom tijelu ili se od njih zaprimaju.

(2) Uz podatak iz stava 1. ovoga člana koji se dostavlja u inostranstvo mora biti sadržano slijedeće upozorenje:

"Ovaj dokument i svi sadržani prilozi smatraju se (navesti stepen tajnosti) i vlasništvo su Bosne i Hercegovine, te se mogu koristiti samo u svrhu za koju su dostavljeni. Primalac dokumenta vodit će brigu o zaštiti tajnosti podataka sadržanih u dokumentu u skladu sa vlastitim propisima o zaštiti tajnih podataka. Dokument i njegov sadržaj ne smije se bez odobrenja Bosne i Hercegovine objavljivati, umnožavati, davati na korištenje drugoj agenciji ili trećoj strani, odnosno koristiti u druge svrhe osim onih zbog koje je dostavljen, a nakon prestanka potrebe za njegovim korištenjem mora se najkasnije do (navesti vremenski rok) uništiti. Bosna i Hercegovina zadržava pravo upita o korištenju dostavljenog dokumenta i podataka koje dokument sadržava, a primalac dokumenta se obavezuje da će o uništenju dokumenta obavijestiti Bosnu i Hercegovine.

(3) Ukoliko je tajni podatak dostavljen drugoj državi na arhivski primjerak ispod oznake stepena tajnosti otiskuje se sigurnosna oznaka "RAZMIJENJEN PODATAK".

(4) Tajni podaci zaprimljeni od međunarodnih organizacija i drugih država se zaštićuju obaveznim otiskivanjem sigurnosne oznake u zavisnosti o sadržaju zaprimljenog dokumenta i to u skladu sa članom 20. Zakona.

Član 46.

(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;

d) VT za stepen tajnosti VRLO TAJNO.

(3) Evidencija iz stava 1. ovog člana sadrži sljedeće rubrike:

redni broj, naziv organa - organizacione jedinice koja je odredila stepen tajnosti, predmet podneska, datum prijema podneska, organizaciona jedinica, klasifikaciona oznaka, ustupljeno drugom organu - datum, promjena stepena tajnosti - datum, prestanak tajnosti - datum, rješen - datum, arhiva - datum, napomena.

(4) Izgled evidencije iz stava 3. ovog člana dat je na obrascu broj 6, koji je sastavni dio ovog Pravilnika.

Član 47.

(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) stepena tajnosti VRLO TAJNO crvena;

b) stepena tajnosti TAJNO žuta;

c) stepena tajnosti POVJERLJIVO plava;

d) stepena tajnosti INTERNO siva.

(2) Omot iz stava 1. ovog člana izrađuje se prema obrascu broj 7, koji čini sastavni dio ovog Pravilnika.

Član 48.

(Spisak uvida)

(1) Svaki organ koji pohranjuje tajne podatke označene stepenom TAJNO ili VRLO TAJNO vodi spisak uvida u kojem se evidentiraju slijedeći podaci:

a) kratak sadržaj predmeta, broj, datum, stepen tajnosti i broj primjerka dokumenta koji sadrži tajni podatak;

b) ime i prezime osobe koja se upoznala sa tajnim podatkom;

c) razlog upoznavanja;

d) datum i vrijeme upoznavanja;

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 49.

(Primjena propisa o arhiviranju)

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

Član 50.

(Pohranjivanje arhivskih primjeraka)

(1) Arhivski primjerak dokumenta označenog stepenom tajnosti TAJNO ili VRLO TAJNO je po pravilu primjerak broj 1. ovlaštenog lica nadležnog organa koji je odredio 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 lica, kojima su primjerci tajnih podataka bili uručeni, spisak uvida, te moguće dozvole za umnožavanje tajnog dokumenta.

Član 51.

(Plan čuvanja)

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

Član 52.

(Sadržaj plana čuvanja)

(1) Plan čuvanja se sastoji od općeg i posebnog dijela.

(2) Opći dio sadrži naročito:

a) procjenu ugroženosti;

b) opis glavnog i pomoćnih objekata (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,

e) mjere čuvanja osoblja koje se bavi tajnim podacima.

(3) Posebni dio sadrži naročito:

a) mjere fizičkog osiguranja (vanjske i unutrašnje fizičko osiguranje, sigurnosne tačke sa opisom zadatka izvođača),

b) mjere tehničkog osiguranja (vanjsko i unutrašnje tehničko osiguranje, kontrola ulaza i izlaza, alarmni sistem i postupke pri aktiviranju pojedinih stepena alarma, dokumentiranje);

c) postupke za nasilno ulaženje i nepredviđene događaje sa planom uništavanja.

(4) Svaki organ mora odrediti odgovornu osobu za izradu plana osiguranja.

(5) Organ može imati i zajednički plan osiguranja za organ i organe u sastavu.

Član 53.

(Provjeravanje efikasnosti plana čuvanja)

(1) Svaki organ će plan čuvanja dopunjavati svakih šest mjeseci.

(2) Plan čuvanja potrebno je najmanje jednom godišnje pregledati te provjeriti efikasnost mjera koje su njime određene.

Član 54.

(Zloupotreba tajnog podatka)

1) Sa svakim neovlaštenim pristupom tajnim podacima, njihovim uništenjem, krađom ili drugim događajem koji ukazuje na zloupotrebu tajnih podataka (u daljnjem tekstu: zloupotreba tajnog podatka) treba odmah upoznati rukovodioca organa odnosno osobu koju je on ovlastio i osigurati sve mjere za onemogućavanje dalje zloupotrebe tajnog podatka te provesti istragu o okolnostima zloupotrebe.

2) Rukovodilac organa u kojem je bio zloupotrebljen podatak mora o tome obavijestiti organ koji je odredio tajni podatak.

3) O svakoj zloupotrebi tajnog podatka treba obavijestiti državni sigurnosni organ.

4) Svaki organ će propisati odgovarajuće postupke i mjere vezano za zloupotrebu tajnih podataka.

Član 55.

(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 podatka, šifru i datum dokumenta, broj kopije vlasnika i kratku sadržinu);

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;

d) postupke i mjere koji su bili izvedeni da se spriječi dalja zloupotreba tajnih podataka.

VI - PRIJELAZNE I ZAVRŠNE ODREDBE

Član 56.

(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 sa članom 86. Zakona.

(2) Na dokumentima iz stava 1. ovog člana precrtat će se stara oznaka stepena tajnosti. Ispod te oznake upisat će se oznaka novog stepena tajnosti te datum i potpis ovlaštene osobe u organu koji je tu promjenu učinio.

Član 57.

(Sigurnosno tehnička oprema)

Sigurnosno tehnička oprema sigurnosnih područja mora odgovarati uvjetima koje na prijedlog državnog sigurnosnog organa odredi Vijeće ministara BiH.

Član 58.

(Završna odredba)

Ovaj Pravilnik stupa na snagu osmog dana od dana objavljivanja u "Službenom glasniku BiH".

VM broj 209/06
31. augusta 2006. Godine
Sarajevo

Predsjedavajući
Vijeća ministara BiH
Adnan Terzić, s. r.

OBRAZAC BROJ 1.

d) STEPEN TAJNOSTI_____
e) PODACI O ORGANU_____
f) IME I PREZIME, _____OVLAŠTENJE BROJ _____OD _____
g) DATUM ODREĐIVANJA STEPENA TAJNOSTI_____
h) NAČIN PRESTANKA_____
i) NAČIN DOSTAVLJANJA_____

UPUTSTVO ZA POPUNJAVANJE OBRASCA:

a. u rubriku «stepen tajnosti» upisuje se jedan od četiri vrste stepena tajnosti (povjerljivo, tajno, itd);
b. u rubriku «podaci o organu» upisuju se podaci o organu čija je ovlaštena osoba odredila stepen tajnosti (naprimjer: Ministarstvo odbrane ili Ministarstvo sigurnosti);
c. u rubriku «ime i prezime i ovlaštenje» upisuje se podatak o osobi koja je u organu odredila stepen tajnosti podatka (naprimjer: N.N. 04-03/05 od 20.05.2010. godine);
d. u rubriku «datum određivanja stepena tajnosti podatka» upisuje se datum kada je određen stepen tajnosti podatka;
e. u rubriku «način prestanka» upisuje se jedan od mogućih načina prestanka tajnosti podatka u skladu sa članom 25. Zakona;
f. u rubriku «način dostavljanja» upisuju se podaci o tome na koji način je izvršena dostava tajnog podatka (naprimjer: kurirom - fizičkom poštom, elektronskom poštom).

OBRAZAC BROJ 2.

a) STEPEN TAJNOSTI_____
b) PODACI O ORGANU_____
c) IME I PREZIME, _____OVLAŠTENJE BROJ _____OD _____
d) DATUM ODREĐIVANJA STEPENA TAJNOSTI_____
e) NAČIN PRESTANKA_____
f) NAČIN DOSTAVLJANJA_____
g) BROJ PRIMJERKA_____
h) UKUPAN BROJ STRANICA DOKUMENTA_____
i) PRILOZI I PRATEĆA DOKUMENTACIJA_____

UPUTSTVO ZA POPUNJAVANJE OBRASCA:

a. u rubriku «stepen tajnosti» upisuje se jedan od četiri vrste stepena tajnosti (povjerljivo, tajno, itd);
b. u rubriku «podaci o organu» upisuju se podaci o organu čija je ovlaštena osoba odredila stepen tajnosti (naprimjer: Ministarstvo odbrane ili Ministarstvo sigurnosti);
c. u rubriku «ime i prezime i ovlaštenje» upisuje se podatak o osobi koja je u organu odredila stepen tajnosti podatka (naprimjer: N.N. 04-03/05 od 20.05.2010. godine);
d. u rubriku «datum određivanja stepena tajnosti podatka» upisuje se datum kada je određen stepen tajnosti podatka;
e. u rubriku «način prestanka» upisuje se jedan od mogućih načina prestanka tajnosti podatka u skladu sa članom 25. Zakona;
f. u rubriku «način dostavljanja» upisuju se podaci o tome na koji način je izvršena dostava tajnog podatka (naprimjer: kurirom, ili poštom);
g. u rubriku «broj primjerka» upisuje se podatak o broju primjerka dokumenta (naprimjer: 5,ili 10 itd....);
h. u rubriku «ukupan broj stranica dokumenta» upisuje se broj stranica dokumenta kao naprimjer: 256 ili 15.....uz napomenu da se samo upisuje broj stranica koje ima dokument;
i. u rubriku «prilozi i prateća dokumentacija» upisuju se podaci o prilozima i pratećoj dokumentaciji koja je pridodata uz dokument kao naprimjer: anex, propratni akt broj 01-01-01 od 10.10.2000 godine itd.

OBRAZAC BROJ 3.

KOPIJA ORIGINALA

a) STEPEN TAJNOSTI_____
b) PODACI O ORGANU _____
c) IME I PREZIME, _____OVLAŠTENJE BROJ _____OD _____
d) DATUM ODREĐIVANJA STEPENA TAJNOSTI_____
e) NAČIN PRESTANKA_____
f) NAČIN DOSTAVLJANJA _____
g) REDNI BROJ KOPIJE_____
h) BROJ I DATUM IZ EVIDENCIJE O UMNOŽAVANJU_____
i) OZNAKA ORGANIZACIONE JEDINICE_____
j) POTPIS SLUŽBENIKA _____

UPUTSTVO ZA POPUNJAVANJE OBRASCA:

a) u rubriku «stepen tajnosti» upisuje se jedan od četiri vrste stepena tajnosti (povjerljivo, tajno, itd);
b) u rubriku «podaci o organu» upisuju se podaci o organu čija je ovlaštena osoba odredila stepen tajnosti (naprimjer: Ministarstvo odbrane ili Ministarstvo sigurnosti);
c) u rubriku «ime i prezime i ovlaštenje» upisuje se podatak o osobi koja je u organu odredila stepen tajnosti podatka (naprimjer: N.N. 04-03/05 od 20.05.2010. godine);
d) u rubriku «datum određivanja stepena tajnosti podatka» upisuje se datum kada je određen stepen tajnosti podatka;
e) u rubriku «način prestanka» upisuje se jedan od mogućih načina prestanka tajnosti podatka u skladu sa članom 25. Zakona;
f) u rubriku «način dostavljanja» upisuju se podaci o tome na koji način je izvršena dostava tajnog podatka (naprimjer: kurirom, ili poštom);
g) u rubriku «redni broj kopije» upisuje se podatak o broju kopije (naprimjer: kopija broj 1 itd);
h) u rubriku «broj i datum iz evidencije o umnožavanju» upisuje se podatak iz evidencije o umnožavanju;
i) u rubriku «oznaka organizacione jedinice» upisuje se podatak o broju ili šifri organizacione jedinice;
j) rubrika «potpis službenika» podrazumjeva potpis lica koje je izvršilo kopiranje.

OBRAZAC BROJ 4.

KOPIJA ORIGINALA

a) STEPEN TAJNOSTI_____
b) PODACI O ORGANU_____
c) IME I PREZIME, _____OVLAŠTENJE BROJ _____OD _____
d) DATUM ODREĐIVANJA STEPENA TAJNOSTI_____
e) NAČIN PRESTANKA_____
f) NAČIN DOSTAVLJANJA_____
g) BROJ PRIMJERKA:_____
h) UKUPAN BROJ STRANICA DOKUMENTA_____
i) PRILOZI I PRATEĆA DOKUMENTACIJA_____
j) REDNI BROJ KOPIJE_____
k) BROJ I DATUM IZ EVIDENCIJE O UMNOŽAVANJU_____
l) OZNAKA ORGANIZACIONE JEDINICE_____
m) POTPIS SLUŽBENIKA _____

UPUTSTVO ZA POPUNJAVANJE OBRASCA:

a) u rubriku «stepen tajnosti» upisuje se jedan od četiri vrste stepena tajnosti (povjerljivo, tajno, itd);
b) u rubriku «podaci o organu» upisuju se podaci o organu čija je ovlaštena osoba odredila stepen tajnosti (naprimjer: Ministarstvo odbrane ili Ministarstvo sigurnosti);
c) u rubriku «ime i prezime i ovlaštenje» upisuje se podatak o osobi koja je u organu odredila stepen tajnosti podatka (naprimjer: N.N. 04-03/05 od 20.05.2010. godine);
d) u rubriku «datum određivanja stepena tajnosti podatka» upisuje se datum kada je određen stepen tajnosti podatka;
e) u rubriku «način prestanka» upisuje se jedan od mogućih načina prestanka tajnosti podatka u skladu sa članom 25. Zakona;
f) u rubriku «način dostavljanja» upisuju se podaci o tome na koji način je izvršena dostava tajnog podatka (naprimjer: kurirom, ili poštom);
g) u rubriku «broj primjerka» upisuje se podatak o broju primjerka dokumenta (naprimjer: 5,ili 10 itd....);
h) u rubriku «ukupan broj stranica dokumenta» upisuje se broj stranica dokumenta kao naprimjer: 256 ili 15.....uz napomenu da se samo upisuje broj stranica koje ima dokument;
i) u rubriku «prilozi i prateća dokumentacija» upisuju se podaci o prilozima i pratećoj dokumentaciji koja je pridodata uz dokument kao naprimjer: anex, propratni akt broj 01-01-01 od 10.10.2000 godine itd.

OBRAZAC BROJ 5.

Na osnovu člana 43. Pravilnika o načinu i obliku oznaka tajnosti podataka, te fizičkim, organizacijskim, tehničkim mjerama i postupcima za čuvanje tajnih podataka («Službeni glasnik BiH» broj_____), rukovodilac organa_____ (navesti konkretano naziv rukovodioca), i z d a j e

KURIRSKO UVJERENJE

Ovim uvjerenjem se potvrđuje da je _____ vlasnik lk broj _____, te đa je službenik_____(upisati naziv organizacije). _____je imenovan za službenog kurira _____(navesti ime institucije) i ovlašten je da nosi pošiljku službenih dokumenta _____(navesti organizaciju čija se pošiljka nosi).

Ovo uvjerenje važi do_____

Datum: Ime, prezime i potpis službenika koji daje ovlaštenje:

Službeni pečat

OBRAZAC BROJ 6.

redni broj, naziv organa – organizacione jedinice koja je odredila stepen tajnosti, predmet podneska, datum prijema podneska, organizaciona jedinica, klasifikaciona oznaka, ustupljeno drugom organu - datum, promjena stepena tajnosti – datum, prestanak tajnosti – datum, riješen – datum, arhiva – datum, napomena.

Redni broj	Naziv	Predmet podneska	Datum prijema	Organizaciona	Klasifikaciona	Ustupljeno	Promjena stepena	Prestanak	Riješen - datum	Arhiva - datum	napomena	

INTERNO

OVO JE OMOT SPISA
ZA
INFORMACIJU SA OZNAKOM TAJNOSTI

SVA LICA KOJA RASPOLAŽU OVOM INFORMACIJOM SU DUŽNA DA ONEMOGUĆE NEOVLAŠTENO OTKRIVANJE ISTE ŠTO JE U INTERESU SIGURNOSTI BOSNE I HERCEGOVINE.

POSTUPANJE, POHRANJIVANJE, UMNOŽAVANJE I RASPOLAGANJE PRILOŽENIM DOKUMENTOM MORA BITI USKLAĐENO SA PRIMJENJIVIM ZAKONIMA, POLITIKAMA, NAREDBAMA I IMPLEMENTIRAJUĆIM REGULATORNIM SMJERNICAMA DATE ORGANIZACIJE.

INTERNO

POVJERLJIVO

OVO JE OMOT SPISA
ZA
INFORMACIJU SA OZNAKOM TAJNOSTI

SVA LICA KOJA RASPOLAŽU OVOM INFORMACIJOM SU DUŽNA DA ONEMOGUĆE NEOVLAŠTENO OTKRIVANJE ISTE ŠTO JE U INTERESU DRŽAVNE SIGURNOSTI BOSNE I HERCEGOVINE.

POSTUPANJE, POHRANJIVANJE, UMNOŽAVANJE I RASPOLAGANJE PRILOŽENIM DOKUMENTOM MORA BITI USKLAĐENO SA PRIMJENJIVIM ZAKONIMA, POLITIKAMA, NAREDBAMA I IMPLEMENTIRAJUĆIM REGULATORNIM SMJERNICAMA DATE ORGANIZACIJE.

POVJERLJIVO

TAJNO

OVO JE OMOT SPISA
ZA
INFORMACIJU SA OZNAKOM TAJNOSTI

SVA LICA KOJA RASPOLAŽU OVOM INFORMACIJOM SU DUŽNA DA ONEMOGUĆE NEOVLAŠTENO OTKRIVANJE ISTE ŠTO JE U INTERESU DRŽAVNE SIGURNOSTI BOSNE I HERCEGOVINE.POSTUPANJE,

POHRANJIVANJE, UMNOŽAVANJE I RASPOLAGANJE PRILOŽENIM DOKUMENTOM MORA BITI USKLAĐENO SA PRIMJENJIVIM ZAKONIMA, POLITIKAMA, NAREDBAMA I IMPLEMENTIRAJUĆIM REGULATORNIM SMJERNICAMA DATE ORGANIZACIJE.

TAJNO

VRLO TAJNO

OVO JE OMOT SPISA
ZA
INFORMACIJU SA OZNAKOM TAJNOSTI

SVA LICA KOJA RASPOLAŽU OVOM INFORMACIJOM SU DUŽNA DA ONEMOGUĆE NEOVLAŠTENO OTKRIVANJE ISTE ŠTO JE U INTERESU DRŽAVNE SIGURNOSTI BOSNE I HERCEGOVINE.

POSTUPANJE, POHRANJIVANJE, UMNOŽAVANJE I RASPOLAGANJE PRILOŽENIM DOKUMENTOM MORA BITI USKLAĐENO SA PRIMJENJIVIM ZAKONIMA, POLITIKAMA, NAREDBAMA I IMPLEMENTIRAJUĆIM REGULATORNIM SMJERNICAMA DATE ORGANIZACIJE.

VRLO TAJNO