Broj: 09-29-1-3231/2016
Sarajevo, 2.12.2016. godine

svi sudovi i tužilaštva u Bosni i Hercegovini
n/r predsjednika sudova i glavnih tužilaca

**Predmet: Politika sigurnosti pravosudnog informacionog sistema Bosne i Hercegovine**

Poštovani,

Visoko sudsko i tužilačko vijeće Bosne i Hercegovine (VSTV BiH) je na sjednici održanoj 8. i 9.11.2016. godine usvojilo Politiku sigurnosti pravosudnog informacionog sistema Bosne i Hercegovine (Politika sigurnosti).

Politika sigurnosti predstavlja rezultat aktivnosti usmjerenih na jačanje sigurnosti pravosudnog informacionog sistema i u njemu pohranjenih podataka. Ista predstavlja krovni dokument kojim se uređuje upravljanje sigurnošću pravosudnog informacionog sistema Bosne i Hercegovine i istovremeno utvrđuju minimalna obavezujuća pravila koja se odnose na postupanje, pristup, obradu, čuvanje i prenos podataka unutar pravosudnog informacionog sistema. Politika sigurnosti istovremeno ima za cilj podići nivo svijesti zaposlenih u pravosuđu o značaju zaštite informacija i unaprijediti njihova znanja o primjeni principa informacione sigurnosti, te osigurati adekvatnu zaštitu od mogućih rizika po pravosudni informacioni sistem i u njemu pohranjene informacije.

Usvajanje Politike sigurnosti predstavlja važan i neophodan korak u uspostavljanju sveobuhvatnog sistema zaštite pravosudnog informacionog sistema i njegovih resursa, a posebno podataka koji se pomoću njega čuvaju i obrađuju od nepoželjnih događaja koji mogu naštetiti integritetu, efikasnosti i ugledu kako pojedinačnih pravosudnih institucija, tako i pravosuđa u BiH u cijelosti.

U svrhu olakšavanja primjene Politike sigurnosti i upoznavanja svih korisnika pravosudnog informacionog sistema s njenim odredbama, Odjel za IKT je osigurao dostupnost Politike sigurnosti putem Internet (wiki) portala, te će u narednom periodu na isti način osigurati dostupnost svih relevantnih dokumenata i resursa koji proizlaze iz Politike sigurnosti.

S poštovanjem,

Predsjednik

MP

Milan Tegeltija

Prilog:

- Politika sigurnosti pravosudnog informacionog sistema Bosne i Hercegovine

Na osnovu člana 17. tačka (24) Zakona o Visokom sudskom i tužilačkom vijeću Bosne i Hercegovine (Službeni glasnik BiH, br. 25/04, 93/05, 48/07, 15/08), a u skladu sa članom 91. stav (2) Pravilnika o unutrašnjem sudskom poslovanju Bosne i Hercegovine (Službeni glasnik BiH, br. 66/12, 40/14), članom 91. stav (2) Pravilnika o unutrašnjem sudskom poslovanju Federacije Bosne i Hercegovine i Brčko distrikta Bosne i Hercegovine (Službeni glasnik BiH, br. 66/12, 40/14) i članom 91. stav (3) Pravilnika o unutrašnjem sudskom poslovanju Republike Srpske (Službeni glasnik RS, broj 9/14), Visoko sudsko i tužilačko vijeće Bosne i Hercegovine, na sjednici održanoj 8. i 9.11.2016. donijelo

# POLITIKU SIGURNOSTI
# PRAVOSUDNOG INFORMACIONOG SISTEMA
# BOSNE I HERCEGOVINE

## POGLAVLJE I - OPŠTE ODREDBE

### *Član 1.*
### *(Predmet)*

(1) Politikom sigurnosti pravosudnog informacionog sistema Bosne i Hercegovine (u daljem tekstu: Politika sigurnosti) se:

a) uređuje upravljanje sigurnošću pravosudnog informacionog sistema Bosne i Hercegovine (u daljem tekstu pravosudni informacioni sistem);

b) utvrđuju minimalna obavezujuća pravila koja se odnose na postupanje, pristup, obradu, čuvanje, prenos i uništenja podataka unutar pravosudnog informacionog sistema.

### *Član 2.*
### *(Svrha)*

Politika sigurnosti predstavlja osnov i okvir za uspostavljanje i razvijanje sistema za upravljanje sigurnošću pravosudnog informacionog sistema, sa ciljem da se:

a) osigura adekvatna zaštita od mogućih unutrašnjih, vanjskih, namjernih ili slučajnih rizika, te ugrožavanja pravosudnog informacionog sistema i u njemu pohranjenih informacija;

b) dâ pregled osnovnih načela sigurnosti informacija;

c) utvrde smjernice za provođenje aktivnosti na planu zaštite informacija;

d) podigne nivo svijesti zaposlenih o značaju zaštite informacija.

### *Član 3.*
### *(Ciljevi)*

Ciljevi Politike sigurnosti su:

a) sprečavanje neovlaštenog pristupa resursima pravosudnog informacionog sistema i u njima pohranjenim informacijama, njihovog uništenja, otuđenja ili otkrivanja neovlaštenim licima;

b) osiguranje povjerljivosti i integriteta informacija, hardvera, softverskih rješenja, mrežne opreme, mrežnih usluga i informaciono-komunikacione infrastrukture (u daljem tekstu IKT infrastruktura);

c) osiguranje dostupnosti resursa pravosudnog informacionog sistema i u njima pohranjenim informacijama;

d) podizanje nivoa svijesti i odgovornosti zaposlenih u pravosuđu Bosne i Hercegovine i njihovo stalno osposobljavanje u vezi sa informacionom sigurnošću;

e) smanjivanje rizika od ljudskih grešaka, krađe, prevare ili zloupotrebe uređaja, sigurnosnih incidenata i kvarova;

f) usvajanje i provođenje dobre prakse u oblasti zaštite elektronski pohranjenih informacija;

g) osiguranje usklađenosti korištenja pravosudnog informacionog sistema sa pozitivnim propisima u Bosni i Hercegovini i relevantnim standardima.

*Član 4.*
*(Obim primjene)*

Politika sigurnosti pravosudnog informacionog sistema se primjenjuje na:

a) članove Visokog sudskog i tužilačkog vijeća Bosne i Hercegovine (u daljem tekstu VSTV-a), sudije i tužioce, sve zaposlene u VSTV-u , kao i sudovima i tužilaštvima u Bosni i Hercegovini, vanjske saradnike, te ovlaštene korisnike u drugim institucijama;

b) objekte VSTV-a i svih sudova i tužilaštava u Bosni i Hercegovini;

c) lokalne računarske mreže (u daljem tekstu LAN mreža) i pravosudnu mrežu širokog područja (u daljem tekstu pravosudna WAN mreža) u Bosni i Hercegovini;

d) datoteke, baze podataka, sistemsku dokumentaciju, korisničke priručnike, radne postupke, softverska rješenja (sistemska, aplikativna, razvojni alati itd.);

e) računarsku opremu, komunikacionu opremu, prenosne medije, tehničku opremu za IKT infrastrukturu (sistemi za napajanje, uređaji za klimatizaciju itd.);

f) usluge i ponude: računarske opreme, komunikacione opreme, softvera, tehničke opreme za IKT infrastrukturu;

g) druge sigurnosne aspekte, kao što su: sigurnost informacija pohranjenih izvan pravosudnog informacionog sistema, zaštita na radu, sigurnost finansijskih transakcija i drugo, čija zloupotreba može ugroziti sigurnost pravosudnog informacionog sistema.

*Član 5.*
*(Odgovornost za primjenu)*

(1) Direktor Sekretarijata VSTV-a u VSTV-u, predsjednici sudova i glavni tužioci (u daljem tekstu: rukovodioci pravosudnih institucija) u pravosudnim institucijama preduzimaju organizacione mjere, te obezbjeđuju finansijske, kadrovske i druge resurse i sredstva potrebna za funkcionisanje pravosudnog informacionog sistema u skladu sa svojim ovlaštenjima i odredbama Politike sigurnosti.

(2) Odjel za informaciono-komunikacionu tehnologiju Sekretarijata VSTV-a (u daljem tekstu: Odjel za IKT) i službenici za informaciono-komunikacionu tehnologiju u pravosudnim institucijama (u daljem tekstu: IKT službenici) su zaduženi za provođenje tehničkih mjera za funkcionisanje pravosudnog informacionog sistema u skladu sa odredbama Politike sigurnosti.

(3) Odjel za IKT i IKT službenici provode mjere predviđene Politikom sigurnosti, prema područjima odgovornosti iz člana 14. Politike sigurnosti.

(4) Svi zaposleni u VSTV-u, sudovima i tužilaštvima, kao i svi vanjski saradnici ovih institucija obavezni su pridržavati se odredbi Politike sigurnosti.

(5) Svi zaposleni u VSTV-u, sudovima i tužilaštvima, kao i svi vanjski saradnici ovih institucija, dužni su da s najvišim stepenom pažnje postupaju sa podacima, informacijama i resursima pravosudnog informacionog sistema, kao i da provode mjere i postupke predviđene Politikom sigurnosti i drugim relevantnim zakonima i podzakonskim aktima iz oblasti zaštite podataka koji se primjenjuju u pravosuđu Bosne i Hercegovine.

***Član 6.***
***(Definicije pojmova)***

(1) Informaciono-komunikaciona tehnologija (IKT) obuhvata sve tehnologije i resurse koji korisnicima omogućavaju prikupljanje, obradu, skladištenje, prenos i korištenje podataka i informacija, kao i upravljanje informacionim sistemima.

(2) IKT oprema predstavlja hardversku komponentu informacionog sistema.

(3) Hardver (engl. hardware) predstavlja skup fizičkih dijelova koji čine neki računarski ili komunikacioni sistem. Hardver obuhvata sve elektronske, električne, elektromehaničke i mehaničke komponente nekog sistema.

(4) Softver (engl. software) predstavlja skup sistemskih i aplikativnih programa koji zajedno omogućavaju hardveru da izvršava zadane zadatke.

(5) Radna stanica je svaki stoni, prenosni ili virtuelni računar u vlasništvu VSTV-a i pravosudnih institucija koji se koristi za obavljanje poslova i zadataka iz nadležnosti VSTV-a i pravosudnih institucija.

(6) LAN mreža (engl. local area network) je lokalna računarska mreža koja omogućava korisnicima dijeljenje resursa na ograničenom prostoru, npr. u okviru jedne zgrade.

(7) Pravosudna WAN mreža (engl. wide area network) je mreža koja povezuje sve LAN mreže pravosudnih institucija u jednu jedinstvenu mrežu.

(8) Nosači podataka su sredstva za trajno ili privremeno čuvanje podataka.

(9) Zlonamjerni program je bilo koji softver koji je, najčešće bez znanja korisnika, ubačen u sistem s namjerom kompromitovanja povjerljivosti, integriteta ili raspoloživosti korisnikovih podataka, aplikacija ili operativnog sistema, ili na neki drugi način uznemirava ili ometa korisnika.

(10) Internet je javna globalna računarska mreža koja povezuje veliki broj računara i računarskih mreža širom svijeta. Internet omogućava korisnicima pristup informacijama, njihovu međusobnu razmjenu, kao i korištenje različitih usluga.

(11) VPN (engl. virtual private network) je tehnologija koja omogućava korisnicima na udaljenim lokacijama uspostavu sigurne komunikacije putem manje sigurne javne ili privatne mreže.

(12) Streaming je tehnologija distribuiranja audio i video sadržaja. Označava prijem i istovremeno reprodukovanje primljenog sadržaja putem računarske mreže.

(13) Elektronska pošta je servis koji omogućava razmjenu elektronskih poruka između pošiljaoca i jednog ili više primalaca.

(14) Dnevnički zapis (engl. log file) predstavlja datoteku u kojoj se automatski evidentiraju informacije o događajima koji se javljaju u toku rada sistema i servisa.

(15) Server soba je zaštićeni prostor u kojem se nalazi informaciono-komunikaciona oprema koja omogućava funkcionisanje pravosudnog informacionog sistema.

(16) Zaštićeni prostor je prostor s ograničenim pristupom unutar VSTV-a odnosno pravosudne institucije koji je obuhvaćen mjerama pojačane fizičke i tehničke zaštite.

(17) Data centar pravosudnog informacionog sistema je server soba u VSTV-u odnosno pravosudnoj instituciji u kojoj su smješteni ključni resursi pravosudnog informacionog sistema.

(18) Informacioni sistem je integrisani set hardverskih i softverskih komponenti za prikupljanje, obradu, skladištenje, prenos i korištenje podataka i informacija.

(19) Pravosudni informacioni sistem Bosne i Hercegovine je integrisani set hardverskih i softverskih komponenti za prikupljanje, obradu, skladištenje, prenos i korištenje podataka i informacija u VSTV-u i pravosudnim institucijama u Bosni i Hercegovini. Pravosudni informacioni sistem obuhvata sve sisteme čije korištenje vodi, koordinira i nadgleda VSTV.

(20) Resursi informacionog sistema podrazumijevaju svu opremu za prikupljanje, obradu, skladištenje, prenos i korištenje podataka i informacija, sav softver (sistemski i aplikativni), opremu za povezivanje na LAN i pravosudnu WAN mrežu, opremu za zaštitu mreže od neovlaštenog upada, detekciju i prevenciju upada, telekomunikacionu oprema, te pasivne instalacije LAN mreža i telekomunikacionih sistema.

(21) Servis informacionog sistema predstavlja skup resursa informacionog sistema međusobno povezanih kako bi korisnicima obezbijedili određene funkcionalnosti.

(22) Katalog servisa je dokument koji sadrži informacije o svim servisima pravosudnog informacionog sistema, uključujući: ime servisa, njegov tip, kategoriju i namjenu, resurse od kojih se sastoji, podatke o osobama odgovornim za njegovo administriranje i druge relevantne informacije.

(23) Izjava o povjerljivosti je dokument čijim se potpisivanjem korisnik sistema obavezuje na trajno čuvanje povjerljivosti podataka s kojima dolazi u kontakt.

(24) Povjerljivost u smislu informacione sigurnosti podrazumijeva osiguravanje zaštite službenih, ličnih, tajnih i drugih osjetljivih podataka i informacija.

(25) Integritet podataka podrazumijeva osiguravanje tačnosti i cjelovitosti podataka tokom njihovog životnog ciklusa.

(26) Princip "najmanjih privilegija" je princip dodjele prava pristupa podacima, informacijama i resursima u obimu koji je korisniku neophodan za izvršavanje povjerenog posla.

(27) Plan oporavka (engl. disaster recovery plan) je skup propisanih procedura koje treba da osiguraju kontinuitet poslovnih procesa u slučaju nekog vanrednog događaja.

(28) Vanredni događaj predstavlja neželjeni, nenamjerni, namjerni ili neočekivani događaj ili niz takvih događaja, koji za posljedicu ima prekid kontinuiteta poslovnih procesa djelimično ili u potpunosti.

(29) Backup resursa i podataka je proces kreiranja rezervnih kopija resursa i podataka, koje se mogu koristiti za rekonstrukciju resursa i podataka u slučaju njihovog oštećenja ili gubitka.

(30) Upravljanje promjenama je proces koji obuhvata planiranje, implementaciju i ocjenu promjena u okviru pravosudnog informacionog sistema. Ovaj proces treba da osigura standardizaciju metoda i postupaka za efikasno i brzo uvođenje promjena, a s ciljem smanjenja uticaja promjena na korisnike pravosudnog informacionog sistema.

(31) Dokumentacija pravosudnog informacionog sistema obuhvata pisanu i elektronsku građu u kojoj su detaljno opisani resursi pravosudnog informacionog sistema s ciljem da se olakša proces njihovog administriranja.

(32) Dnevnik ulazaka je evidencija svih pristupa server sobama u VSTV-u odnosno pravosudnoj instituciji.

(33) IKT službenik je uposlenik pravosudne institucije koji u okviru poslova u pravosudnoj instituciji vrši nadzor, održavanje, upravljanje i administriranje dijela pravosudnog informacionog sistema u matičnoj instituciji u okviru svojih nadležnosti. IKT službenik ima ulogu administratora u matičnoj instituciji.

(34) Administrator je korisnik pravosudnog informacionog sistema koji obavlja poslove vezane za nadzor, održavanje, upravljanje i administriranje jednim ili više resursa pravosudnog informacionog sistema. Administrator je korisnik sa najvećim ovlaštenjima nad konkretnim resursom pravosudnog informacionog sistema.

(35) Nadležni administrator je administrator Odjela za IKT, odnosno IKT službenik pravosudne institucije nadležan za resurs pravosudnog informacionog sistema.

(36) Službenik za informacionu sigurnost je osoba koja se bavi svim aspektima sigurnosti informacionog sistema (kontrola sprovođenja sigurnosnih mjera, nadzor sistema, analiza sigurnosnih incidenata, analiza potencijalnih prijetnji i prevencija, unapređenje sigurnosti sistema) s ciljem obezbjeđenja povjerljivosti, integriteta i raspoloživosti resursa, servisa, podataka i informacija.

(37) Administratorski nalog je korisnički nalog administratora jednog ili više resursa pravosudnog informacionog sistema. Administratorski nalog omogućava obavljanje poslova u okviru uloge administratora nad konkretnim resursom.

(38) Administrativni nalog je generički ili zadani nalog koji nije vezan za individualnog korisnika, a služi za administriranje resursa pravosudnog informacionog sistema.

(39) Servisni nalog je generički ili zadani nalog koji nije vezan za individualnog korisnika, a služi za administriranje servisa pravosudnog informacionog sistema.

(40) Korisnički nalog je skup podataka namijenjen identifikaciji korisnika u pravosudnom informacionom sistemu i autorizaciji pristupa resursima i servisima pravosudnog informacionog sistema.

(41) Šifra je niz znakova koji se koristi za autentikaciju korisnika u svrhu dokazivanja identiteta i potvrde ovlaštenja korisnika za pristup resursima i servisima pravosudnog informacionog sistema.

(42) Autentikacija je proces utvrđivanja identiteta korisnika sistema, najčešće na osnovu korisničkog imena i šifre.

(43) Pravosudne institucije su svi sudovi i tužilaštva nad kojima VSTV BiH ima nadležnosti definisane Zakonom o VSTV BiH.

(44) Odjel za AKP je Odjel za administraciju i kadrovsku politiku pri Sekretarijatu VSTV-a BiH.

(45) Odjel za IKT je Odjel za informaciono-komunikacionu tehnologiju pri Sekretarijatu VSTV-a BiH.

***Član 7.***
***(Nadzor nad primjenom Politike sigurnosti)***

Nadzor nad provođenjem Politike sigurnosti vrši VSTV, u skladu sa svojim nadležnostima.

***Član 8.***
***(Odstupanja od primjene Politike sigurnosti)***

(1) Radi otklanjanja teškoća u funkcionisanju pravosudnog informacionog sistema dozvoljena su određena odstupanja, suspenzije ili izuzeci od primjene Politike sigurnosti.

(2) Zahtjev za odstupanje, suspenziju ili izuzetak iz stava (1) ovog člana rukovodilac pravosudne institucije ili od njega ovlaštena osoba, glavni disciplinski tužilac, šef odjela u Sekretarijatu VSTV-a, (u daljem tekstu: Sekretarijat) odnosno zamjenik šefa Odjela za IKT, upućuje šefu Odjela za IKT.

(3) Nakon što šef Odjela za IKT, u saradnji sa zamjenicima i drugim zaposlenim u Odjelu za IKT, izvrši analizu mogućeg uticaja predloženih odstupanja, suspenzija ili izuzetaka od primjene Politike sigurnosti na sigurnost pravosudnog informacionog sistema, istu dostavlja direktoru Sekretarijata na razmatranje i odlučivanje.

(4) Odjel za IKT je dužan informisati podnosioca zahtjeva o odobrenom odstupanju, suspenziji ili izuzetku iz stava (2) ovog člana.

(5) Zahtjevi i odobrenja u vezi sa odstupanjem, suspenzijom ili izuzetkom obavezno se dokumentuju prema proceduri koju donosi direktor Sekretarijata.

## POGLAVLJE II – PRAVOSUDNI INFORMACIONI SISTEM

***Član 9.***
***(Katalog servisa)***

(1) Direktor Sekretarijata, na prijedlog šefa Odjela za IKT, odlukom utvrđuje katalog servisa pravosudnog informacionog sistema koji su u nadležnosti VSTV-a, te određuje poslovni značaj i odgovorne osobe za upravljanje svakim pojedinačnim servisom.

(2) Rukovodilac pravosudne institucije odlukom utvrđuje katalog servisa pravosudnog informacionog sistema koji su u nadležnosti pravosudne institucije, te određuje poslovni značaj i odgovorne osobe za upravljanje svakim pojedinačnim servisom.

(3) Katalog iz st. (1) i (2) ovog člana se redovno ažurira.

### *Član 10.*
### *(Korisnici pravosudnog informacionog sistema)*

Korisnici pravosudnog informacionog sistema su sudije, tužioci i drugi zaposleni u svim sudovima i tužilaštvima u Bosni i Hercegovini, članovi VSTV-a, zaposleni u VSTV-u, zaposleni u centrima za edukaciju sudija i tužilaca, ovlašteni korisnici u drugim institucijama, te fizička i pravna lica koja koriste servise pravosudnog informacionog sistema.

### *Član 11.*
### *(Razvoj pravosudnog informacionog sistema)*

(1) Razvoj pravosudnog informacionog sistema predstavlja aktivnosti na unapređenju sistema kako bi se osigurala njegova usklađenost sa najnovijim tehnološkim rješenjima i standardima, izmjenama propisa koji regulišu rad pravosuđa, te odgovorilo potrebama efikasnijeg, kvalitetnijeg, odgovornijeg i transparentnijeg rada pravosuđa u Bosni i Hercegovini, pri tome posebno vodeći računa o aspektu sigurnosti.

(2) VSTV usvaja strateške politike razvoja pravosudnog informacionog sistema na osnovu prijedloga iz stava (3) ovog člana.

(3) Posebno radno tijelo, kojeg formira VSTV, zaduženo je za pripremu prijedloga iz oblasti strateškog planiranja i razvoja pravosudnog informacionog sistema. Stručnu podršku radnom tijelu pruža Odjel za IKT i po potrebi, drugi odjeli Sekretarijata.

(4) Pri formiranju radnog tijela iz stava (3) ovog člana vodi se računa o zastupljenosti stručnjaka za relevantne pravne i informatičke oblasti, uključujući predstavnike sudske i tužilačke uprave, te o regionalnoj zastupljenosti pravosudnih institucija.

(5) Radno tijelo iz stava (3) ovog člana je dužno osigurati uključenost korisnika iz svih sudova i tužilaštava u proces prikupljanja korisničkih prijedloga za unapređenje i dalji razvoj pravosudnog informacionog sistema.

(6) Odjel za IKT priprema projektne prijedloge i prateću tehničku dokumentaciju, te vrši tehničku implementaciju projekata razvoja pravosudnog informacionog sistema i dokumentovanje sistema u skladu sa važećim internim aktima VSTV-a.

(7) Rukovodioci pravosudnih institucija su dužni osigurati organizacione i kadrovske preduslove za nesmetano provođenje projekata razvoja pravosudnog informacionog sistema koje odobri VSTV, od faze planiranja do faze implementacije u pravosudnim institucijama kojima rukovode.

### *Član 12.*
### *(Principi upravljanja promjenama u pravosudnom informacionom sistemu)*

(1) Upravljanje promjenama u okviru pravosudnog informacionog sistema vrši se u skladu sa sljedećim principima:

a) promjene moraju biti odobrene od strane šefa Odjela za IKT ili zamjenika kojeg on ovlasti;

b) o promjenama se obavještavaju sve osobe odgovorne za područja na koja će promjene imati uticaja, kako bi se sa njima usaglasile i uskladile potrebne mjere i postupci;

c) prije provođenja promjena provode se kontrole i postupci za provjeru pravilnosti funkcionisanja pravosudnog informacionog sistema nakon promjena;

d) utvrđuje se da li je potrebno izmijeniti i dopuniti pravne akte;

e) provjerava se da li je potrebno dodatno prilagođavanje nekog od dijelova sistema (aplikacije, baze podataka, mrežne konfiguracije, datoteke itd.);

f) eventualno instaliranje IKT opreme mora da bude izvedeno u skladu sa uputstvima proizvođača odnosno dobavljača, te pravilima struke;

g) sve promjene i nadgradnje se prethodno testiraju;

h) obavezno se ostavlja mogućnost za vraćanje sistema u prethodno funkcionalno stanje;

i) u svim postupcima promjena i nadgradnje vodi se dnevnik rada i obezbjeđuje se ažuriranje sistemske dokumentacije;

j) u slučaju promjena koje su od uticaja na rad korisnika neposredni korisnici se pravovremeno obavještavaju o uvođenju promjene, njenoj svrsi i eventualnom uticaju na njihov rad, a u slučaju potrebe organizuje se i njihova dodatna edukacija.

(2) Postupak upravljanja promjenama iz stava (1) ovog člana će biti regulisan posebnim uputstvom koje donosi direktor Sekretarijata na prijedlog šefa Odjela za IKT.

***Član 13.***
***(Administriranje i održavanje pravosudnog informacionog sistema)***

(1) Administriranje pravosudnog informacionog sistema je kontinuirana djelatnost koja podrazumijeva instaliranje, konfigurisanje, testiranje i nadzor svih komponenti sistema s posebnim naglaskom na sigurnost.

(2) Pod održavanjem pravosudnog informacionog sistema podrazumijeva se instaliranje hardverskih komponenti i otklanjanje hardverskih kvarova na svim komponentama sistema, te obnavljanje i ažuriranje softverskih komponenti sistema.

***Član 14.***
***(Podjela odgovornosti za administriranje pojedinih resursa pravosudnog informacionog sistema)***

(1) Odjel za IKT je nadležan za administriranje resursa uspostavljenih pod nadzorom VSTV-a, i to:

a) sistema za autentikaciju korisnika i infrastrukturnih servisa smještenih u data centrima, sudovima i tužilaštvima;

b) servera elektronske pošte smještenih u data centrima, sudovima i tužilaštvima;

c) web servera, servera baza podataka i aplikacijskih servera smještenih u data centrima, sudovima i tužilaštvima;

d) servera za upravljanje zaštitom od zlonamjernih programa i neželjene elektronske pošte smještenih u data centrima;

e) servera za upravljanje izradom rezervnih kopija resursa i podataka (u daljem tekstu backup) smještenih u data centrima;

f) sistema za nadzor pravosudne WAN mreže, te LAN mreže i mrežnih servisa u data centrima;

g) opreme za povezivanje na pravosudnu WAN mrežu smještene u data centrima, sudovima i tužilaštvima;

h) svih ostalih servisa navedenih u katalogu servisa VSTV-a.

(2) IKT službenik u matičnoj pravosudnoj instituciji administrira:

a) korisničke naloge za sudije/tužioce i ostalo osoblje;

b) naloge radnih stanica i dijeljenih štampača;

c) lokalne servere datoteka (u daljem tekstu file serveri);

d) radne stanice i servere štampača;

e) web servere, servere baza podataka i aplikacijske servere smještene u sudovima i tužilaštvima za baze podataka i aplikacije koje nisu razvijene pod nadzorom VSTV-a, ukoliko je posebnim propisima ili odlukama njihovo administiranje povjereno IKT službenicima;

f) aktivnu opremu LAN mreže do pristupne tačke na pravosudnu WAN mrežu.

(3) Radi smanjenja mogućnosti neovlaštene izmjene i/ili zloupotrebe podataka i informacija pohranjenih u pravosudnom informacionom sistemu, administriranje svakog pojedinačnog resursa pravosudnog informacionog sistema vrše najmanje dvije osobe.

(4) Ukoliko zahtjev iz stava (3) ovog člana nije moguće ispuniti u okviru postojećih kadrovskih resursa, direktor Sekretarijata, odnosno rukovodilac pravosudne institucije može donijeti odluku o angažovanju spoljnih saradnika odgovarajuće stručnosti.

***Član 15.***
***(Redovni nadzor pravosudnog informacionog sistema)***

(1) Odjel za IKT, odnosno IKT službenik vrši redovni nadzor resursa pravosudnog informacionog sistema za koje je nadležan, isključivo u svrhu održavanja i oporavka sistema, osiguravanja performansi i sigurnosti sistema, te otklanjanja sigurnosnih nedostataka.

(2) Odjel za IKT, odnosno IKT službenik može vršiti elektronski uvid i eventualne izmjene podataka kreiranih, poslanih, primljenih i pohranjenih u pravosudnom informacionom sistemu isključivo na obrazložen zahtjev korisnika u sistemu korisničke podrške, u mjeri u kojoj je to neophodno za rješavanje korisničkog zahtjeva.

***Član 16.***
***(Vanredni nadzor pravosudnog informacionog sistema)***

(1) Vanredni nadzor podrazumijeva elektronski uvid u korisničke podatke kreirane, poslane, primljene i pohranjene u pravosudnom informacionom sistemu i vrši se po pismenom nalogu direktora Sekretarijata, odnosno rukovodioca institucije kojoj pripada korisnik.

(2) Vanredni nadzor vrši Odjel za IKT, odnosno IKT službenik u sljedećim situacijama:

a) istraga o navodima kršenja zakona od strane korisnika;

b) istraga o zloupotrebi ili neprihvatljivom korištenju resursa pravosudnog informacionog sistema od strane korisnika;

c) istraga o narušavanju sigurnosti pravosudnog informacionog sistema;

d) u slučaju nemogućnosti kontaktiranja korisnika, kada se neodložno moraju obaviti određeni poslovi koji zahtijevaju pristup podacima dostupnim samo ovom korisniku, pri čemu nadređeni rukovodilac naknadno mora da obavijesti korisnika o potrebi pristupa podacima.

***Član 17.***
***(Postupanje u slučaju incidenata iz oblasti sigurnosti pravosudnog informacionog sistema)***

(1) Incident iz oblasti sigurnosti pravosudnog informacionog sistema je svaki događaj koji za posljedicu ima narušavanje sigurnosti pravosudnog informacionog sistema, te predstavlja kršenje Politike sigurnosti.

(2) Svaki korisnik koji uoči incident u smislu Politike sigurnosti je dužan bez odlaganja obavijestiti službenika za informacionu sigurnost u VSTV-u, odnosno pravosudnoj instituciji i dostaviti mu sve relevatne informacije vezane za incident, uključujući i raspoložive dnevničke zapise relevantnih resursa informacionog sistema.

(3) Službenik za informacionu sigurnost analizira dostavljene informacije i podnosi izvještaj direktoru Sekretarijata, odnosno rukovodiocu pravosudne institucije. Izvještaj sadrži i prijedlog mjera koje je potrebno preduzeti u cilju rješavanja incidenta.

(4) Na osnovu izvještaja službenika za informacionu sigurnost o incidentu, direktor Sekretarijata, odnosno rukovodilac pravosudne institucije može nadležnom administratoru uputiti nalog za vanredni nadzor iz člana 16. stav 1. Politike sigurnosti ili naložiti preduzimanje drugih tehničkih mjera.

(5) Službenik za informacionu sigurnost može nadležnom administratoru naložiti provođenje privremene mjere zabrane pristupa određenom ili svim resursima pravosudnog informacionog sistema za korisnika za kojeg se sumnja da je prekršio odredbe Politike sigurnosti, ukoliko postoji opravdana sumnja da bi isti mogao ukloniti tragove ili otežati odnosno onemogućiti rješavanje incidenta.

(6) Nadležni administrator je dužan bez odlaganja postupiti prema nalogu iz st (4) i (5) ovog člana. O provedenim aktivnostima ili razlozima za nemogućnost postupanja mora odmah obavijestiti neposredno nadređenog rukovodioca i nalogodavca iz st (4) i (5) ovog člana.

(7) Ako rješavanje incidenta zahtjeva uvid u lične podatke, takav uvid može da obavi samo ovlašteno lice u skladu sa odredbama Zakona o zaštiti ličnih podataka.

(8) Službenik za informacionu sigurnost vodi evidenciju koja sadrži relevantne informacije o incidentima, preduzetim mjerama i načinu njihovog rješavanja. Sadržaj evidencije propisuje direktor Sekretarijata na prijedlog šefa Odjela za IKT.

## POGLAVLJE III - ORGANIZACIONE MJERE SIGURNOSTI PRAVOSUDNOG INFORMACIONOG SISTEMA

***Član 18.***
***(Načela sigurnosti pravosudnog informacionog sistema)***

Sigurnost pravosudnog informacionog sistema temelji se na načelima:

a) integriteta (zaštita podataka i informacija od neautorizovanog pristupa i promjena, obezbjeđenje tačnosti cjelovitosti podataka, informacija i postupaka);

b) povjerljivosti (zaštita službenih, ličnih, tajnih i drugih osjetljivih podataka i informacija);

c) raspoloživosti (osiguranje pristupa podacima, informacijama i resursima svim ovlaštenim korisnicima);

d) stručnosti (od svih zaposlenih i od vanjskih saradnika zahtjeva se visok nivo stručnosti i profesionalnosti).

***Član 19.***
***(Zakonitost i poslovne potrebe)***

Informacije se unutar pravosudnog informacionog sistema mogu koristiti (čitati, zapisivati, mijenjati, prenositi) samo u skladu sa pozitivnim zakonskim i podzakonskim propisima i u mjeri i obimu neophodnom za ispunjenje poslovnih potreba, u skladu sa nadležnostima svake pravosudne institucije.

***Nabavka IKT opreme, softverskih rješenja i usluga***

***Član 20.***
***(Postupak odobravanja nabavke IKT opreme, softverskih rješenja i usluga)***

(1) Svaka nabavka IKT opreme, softverskih rješenja i usluga pokreće se pisanim zahtjevom odgovornog lica u skladu sa internim aktima VSTV-a, odnosno pravosudne institucije koji regulišu provođenje postupaka nabavki.

(2) U procesu podnošenja zahtjeva iz prethodnog stava, podnositelj ima obavezu pribaviti mišljenje Odjela za IKT. Odjel za IKT, odnosno IKT službenik, svako za svoje područje odgovornosti, provjerava zahtjev imajući u vidu postojeću infrastrukturu i softverska rješenja, te podnositelju zahtjeva u VSTV-u odnosno pravosudnoj instituciji dostavlja prijedlog nabavke odnosno tehničku specifikaciju opreme ili softverskog rješenja.

(3) Odluka o pokretanju nabavke, izbor najpovoljnije ponude i plan realizacije nabavke donosi se u skladu sa internim aktima VSTV-a, odnosno pravosudne institucije, koji regulišu provođenje postupaka nabavki.

(4) Odgovorna osoba u Odjelu za IKT, odnosno IKT službenik, sarađuje sa izabranim dobavljačem u toku realizacije ugovora i obezbjeđuje adekvatan poslovni, sigurnosni i tehnološki nadzor u skladu sa Politikom sigurnosti.

***Član 21.***
***(Ugovorno uređenje odnosa sa dobavljačem)***

(1) Zaključenjem ugovora o isporuci opreme ili pružanju usluga koje mogu biti od uticaja na sigurnost pravosudnog informacionog sistema započinje obaveza isporučioca opreme ili pružaoca usluge da postupa u skladu sa Politikom sigurnosti.

(2) U procesu planiranja i provođenja nabavke definišu se sljedeći zahtjevi koje dobavljači moraju ispuniti:

a) opis usluge i predviđeno vrijeme njenog obavljanja; pri opisu usluge se određuju ciljni, mjerljivi i nepromjenljivi nivoi pružanja usluga;

b) nivo neispunjavanja ugovorenih usluga, uključujući njihovo ponavljanje u određenom vremenu koje se tretira kao kršenje ugovora;

c) pravo VSTV-a, odnosno pravosudne institucije za provođenjem pregleda i nadzora nad realizacijom ugovornih obaveza, koje u njihovo ime mogu obavljati i treće osobe;

d) obaveze u vezi s poštivanjem zahtjeva lex specialis propisa, kao što su propisi iz oblasti zaštite podataka i zaštite prava intelektualnog vlasništva;

e) utvrđeni način koordinacije i izvještavanja u procesu realizacije ugovora s posebnim naglaskom na izvještavanje u pogledu otkrivanja i istraživanja sigurnosnih incidenata;

f) drugi zahtjevi potrebni za što preciznije definisanje saradnje između ugovarača i dobavljača.

(3) Kada je za realizaciju nabavke potreban pristup resursima pravosudnog informacionog sistema ili podacima i informacijama pohranjenim u istom, osobe angažovane od strane dobavljača opreme ili izvršioca usluge su dužne potpisati izjavu o trajnom čuvanju povjerljivosti svih podataka i informacija do kojih dođu u toku provođenja postupka nabavke i realizacije ugovora.

(4) Oprema za digitalizaciju, konverziju i čuvanje dokumentarne i arhivske građe koja je predmet nabavke, mora obezbijediti i odgovarajući nivo sigurnosne zaštite, te biti usklađena sa pozitivnim zakonskim i podzakonskim propisima, internim aktima VSTV-a odnosno pravosudne institucije i Politikom sigurnosti.

***Ljudski resursi***

***Član 22.***
***(Dodjela ovlaštenja za pristup resursima, podacima i informacijama u pravosudnom informacionom sistemu)***

(1) Nadležni rukovodeći državni službenik u VSTV-u odnosno rukovodilac pravosudne institucije ili osoba koju on ovlasti, pismenim putem dodjeljuje ili oduzima korisnicima ovlaštenja za pristup resursima, podacima i informacijama u pravosudnom informacionom sistemu.

(2) Ovlaštenja iz stava (1) ovog člana se dodjeljuju po principu "najmanjih privilegija".

(3) Nadležni administrator provodi tehničke mjere dodjele, izmjene i oduzimanja prava pristupa na osnovu ovlaštenja iz stava (1) ovog člana.

(4) Evidenciju prava pristupa iz stava (1) ovog člana vodi i ažurira Odjel za IKT, odnosno IKT službenik, prema sadržaju koji propisuje direktor Sekretarijata odnosno rukovodilac pravosudne institucije.

(5) Najmanje jednom godišnje Odjel za IKT, odnosno IKT službenik, dostavlja izvještaj sa imenima korisnika i njihovim pravima pristupa šefovima unutrašnjih organizacionih jedinica u VSTV-u odnosno pravosudnoj instituciji, koji potvrđuju ili po potrebi predlažu izmjene prava pristupa shodno stavu (1) ovog člana.

(6) Pravilnikom o kategorizaciji, čuvanju i korištenju podataka, koji donosi VSTV odnosno rukovodilac pravosudne institucije, propisuje se kategorizacija podataka, označavanje podataka, dodjeljivanje prava pristupa podacima, rukovanje podacima i katalog podataka u vlasništvu pravosudne institucije.

(7) Sistemi za kreiranje zapisa moraju osigurati precizno određivanje vremena i datuma pristupa i promjene podataka najvišeg stepena osjetljivosti u skladu sa Pravilnikom o kategorizaciji, čuvanju i korištenju podataka iz stava (6) ovog člana.

***Član 23.***
***(Izjava o povjerljivosti)***

(1) Izjavu o povjerljivosti potpisuju svi zaposleni u VSTV-u i pravosudnim institucijama, čime se potvrđuje da je zaposleni upoznat sa Politikom sigurnosti.

(2) Izjava mora biti potpisana prije izdavanja ovlaštenja za pristup resursima, podacima i informacijama u pravosudnom informacionom sistemu.

(3) Izjava o povjerljivosti se evidentira u kadrovskim evidencijama.

(4) Nadležni odjel u Sekretarijatu odnosno pravosudnoj instituciji je odgovoran za uključivanje klauzule povjerljivosti u ugovor sa ugovaračem ili sa vanjskim saradnikom.

***Član 24.***
***(Podizanje svijesti o sigurnosti informacija)***

(1) Osnovno osposobljavanje zaposlenih iz oblasti informacione sigurnosti se izvodi u roku od 3 mjeseca od zasnivanja radnog odnosa.

(2) Osposobljavanje može biti provedeno samoobrazovanjem, prisustvovanjem predavanjima o sigurnosti, korištenjem multimedijalnih i drugih obrazovnih tehnika.

(3) Odjel za AKP, odnosno sudska/tužilačka uprava, je dužna osigurati uslove da se osposobljavanje zaposlenih iz oblasti informacione sigurnosti kontinuirano provodi.

(4) Nadležni iz stava (3) ovog člana su dužni jedanput godišnje provjeriti nivo osposobljenosti zaposlenih iz oblasti informacione sigurnosti i po potrebi isplanirati njihovo dodatno osposobljavanje.

***Član 25.***
***(Zasnivanje radnog odnosa)***

(1) Odjel za AKP, odnosno sudska/tužilačka uprava, će u slučaju zasnivanja radnog odnosa sa novim zaposlenikom odrediti datum aktiviranja prava pristupa resursima, podacima i informacijama u pravosudnom informacionom sistemu, te prava fizičkog pristupa prostorijama, a prema zahtjevu neposredno nadređenog rukovodioca novoga zaposlenika.

(2) Novi zaposlenik će od nadležne organizacione jedinice zadužiti računarsku, telekomunikacionu i kancelarijsku opremu.

***Član 26.***
***(Duža odsutnost zaposlenika)***

(1) U slučaju duže odsutnosti zaposlenika, Odjel za AKP odnosno sudska/tužilačka uprava dužna je elektronskim putem obavijestiti Odjel za IKT, odnosno IKT službenika o potrebnim radnjama i mjerama ograničenja prava pristupa resursima, podacima i informacijama u pravosudnom informacionom sistemu.

(2) Odjel za IKT, odnosno IKT službenik, će obavijestiti Odjel za AKP, odnosno sudsku/tužilačku upravu o provedenim mjerama po osnovu zahtjeva iz stava (1) ovog člana.

***Član 27.***
***(Gubitak ili otuđenje opreme)***

(1) Ukoliko zaposlenik VSTV-a, odnosno pravosudne institucije izgubi povjerenu mu opremu ili mu ista bude otuđena mora o tome bez odlaganja obavijestiti Odjel za AKP, odnosno sudsku/tužilačku upravu.

(2) Zaposlenik iz stava (1) ovog člana dužan je da o gubitku ili otuđenju opreme koja mu je povjerena pribavi potvrdu policije. Potvrda se predaje Odjelu za AKP, odnosno sudskoj/tužilačkoj upravi.

***Član 28.***
***(Prestanak radnog odnosa)***

(1) Odjel za AKP odnosno sudska/tužilačka uprava će u slučaju prestanka radnog odnosa zaposlenika odrediti datum ukidanja prava pristupa resursima, podacima i informacijama u pravosudnom informacionom sistemu, te prava fizičkog pristupa prostorijama, a najkasnije sa danom prestanka radnog odnosa.

(2) Zaposlenik kojem prestaje radni odnos je dužan vratiti svu zaduženu opremu nadležnoj organizacionoj jedinici. Prilikom vraćanja opreme obezbjeđuje se i potvrda odgovorne osobe.

(3) Zaposlenik kojem prestaje radni odnos ili zaposlenik koji se raspoređuje na drugo radno mjesto unutar jedne institucije je dužan predati sve elektronske i neelektronske dokumente nadređenom rukovodiocu.

(4) Zaposleniku kojem prestaje radni odnos nije dozvoljeno kopiranje i iznošenje elektronskih dokumenata iz stava (3) ovog člana.

(5) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije, na zahtjev zaposlenika kojem prestaje radni odnos, može odobriti kopiranje i predaju elektronskih dokumenata koji su označeni stepenom NEOSJETLJIVO tom zaposleniku.

(6) O primopredaji iz st. (3) i (5) ovog člana se sačinjava i potpisuje zapisnik.

(7) U slučaju raspoređivanja na drugo radno mjesto unutar institucije, prethodni i novi neposredno nadređeni rukovodilac će zajednički ustanoviti da li je potrebno zaposleniku omogućiti prenos ovlaštenja za pristup resursima, podacima i informacijama u pravosudnom informacionom sistemu, odnosno da li je potrebno određena ovlaštenja izmijeniti ili ukinuti. Odjel za AKP odnosno sudska/tužilačka uprava je zadužena za izvršenje njihovog zaključka.

***Član 29.***
***(Službenik za informacionu sigurnost)***

(1) Službenik za informacionu sigurnost u VSTV-u, odnosno pravosudnoj instituciji zadužen je za:

a) kontrolu provođenja organizacionih i tehničkih mjera predviđenih Politikom sigurnosti i predlaganje unapređenja iste;

b) izradu nacrta provedbenih akata i propisa predviđenih Politikom sigurnosti;

c) redovno ili ad-hoc izvještavanje direktora Sekretarijata, odnosno rukovodioca pravosudne institucije o svim relevantnim pitanjima iz oblasti informacione sigurnosti;

d) analizu informacija i dostavljanje izvještaja nadležnim rukovodiocima u slučajevima incidenata;

e) izradu programa osposobljavanja zaposlenih iz oblasti informacione sigurnosti.

(2) Ukoliko VSTV, odnosno pravosudna institucija nije u mogućnosti predvidjeti posebno radno mjesto službenika za informacionu sigurnost, poslovi i zadaci iz stava (1) ovog člana će se predvidjeti opisom poslova nekog od već utvrđenih radnih mjesta.

(3) Službenik za informacionu sigurnost poznaje relevantni pravni okvir za zaštitu podataka i informacionu sigurnost, posjeduje neophodan nivo znanja iz oblasti informacionih tehnologija za obavljanje svojih zadataka, te posjeduje visoke moralne standarde.

(4) Službenik za informacionu sigurnost VSTV-a koordinira i daje smjernice za rad službenika za informacionu sigurnost u pravosudnoj instituciji.

## POGLAVLJE IV – FIZIČKE I TEHNIČKE MJERE SIGURNOSTI PRAVOSUDNOG INFORMACIONOG SISTEMA

### *Član 30.*
### *(Fizička i tehnička zaštita server sobe)*

(1) U VSTV-u, odnosno pravosudnoj instituciji se uspostavljaju mjere fizičke i tehničke zaštite u zaštićenom prostoru s ograničenim pristupom – server sobi, u kojoj se nalazi IKT oprema koja omogućava funkcionisanje pravosudnog informacionog sistema.

(2) Opremu za fizičku i tehničku zaštitu čini:

a) video nadzor – instaliran na način da pokriva ulaz i izlaz iz server sobe, radi zaštite opreme koja je od ključnog značaja za nesmetano funkcionisanje pravosudnog informacionog sistema; koristi se samo u svrhe i na način utvrđen Zakonom o zaštiti ličnih podataka;

b) protivprovalni sistem (kartična kontrola pristupa, protivprovalna vrata itd.);

c) sistem mehaničke zaštite (neprobojna stakla, vatrootporni ormari);

d) alarmni uređaji (na ulazu i izlazu iz server sobe).

### *Član 31.*
### *(Servisiranje tehničkih sredstava zaštite server sobe)*

(1) O redovnom održavanju i servisiranju tehničkih sredstava zaštite server sobe stara se pružalac usluge s kojim VSTV odnosno pravosudna institucija ima zaključen ugovor o održavanju.

(2) Po isteku garantnog roka za sva značajnija tehnička sredstva zaključuje se ugovor o održavanju i to najmanje mjesec dana prije isteka garantnog roka.

*Član 32.*
*(Pristup server sobi)*

(1) Server soba je prostor u kojem se provode pojačane mjere nadzora nad pristupom osoba.

(2) Pojačane mjere nadzora se mogu provoditi i u drugim prostorijama u kojima su smještene značajne instalacije i komunikaciona oprema pravosudnog informacionog sistema.

(3) Ulaz u server sobu je dozvoljen samo ovlaštenim zaposlenicima. Ovlaštenje mora biti izdato od strane šefa Odjela za IKT za server sobu VSTV-a odnosno rukovodioca pravosudne institucije za server sobu u pravosudnoj instituciji. Popisi datih ovlaštenja i osoba moraju biti revidirani najmanje jedanput godišnje.

(4) Svaki ulazak u server sobu evidentira se u dnevniku ulazaka, koji vodi odjel za IKT za server sobu VSTV-a odnosno IKT službenik za server sobu u pravosudnoj instituciji. U dnevniku ulazaka evidentira se ovlaštena osoba koja je pristupila server sobi i tačan vremenski period boravka u server sobi. Dnevnici ulazaka svih pravosudnih institucija moraju biti stalno dostupni odjelu za IKT u elektronskom obliku.

(5) Ulaz u server sobu se može odobriti i radnicima ugovornih pružalaca usluga kojima je ulazak u taj prostor potreban radi izvršenja ugovorom preuzetih obaveza. Ovo osoblje ulazi u server sobu po postupku i na način određen ugovorom o vršenju predmetnih radova i usluga, te Politikom sigurnosti.

(6) O svakom ulasku osoba iz stava (5) ovog člana u server sobu obavještava se šef Odjela za IKT za server sobu VSTV-a odnosno rukovodilac pravosudne institucije za server sobu u pravosudnoj instituciji, koji će odrediti zaposlenog koji će vanjskog saradnika pratiti sve vrijeme njegovog boravka, odnosno do izlaska iz VSTV-a odnosno pravosudne institucije. U dnevniku ulazaka evidentira se osoba koja je pristupila server sobi, svrha pristupa, osoba koja je izdala odobrenje za pristup, osoba koja je u pratnji i tačan vremenski period boravka u server sobi.

(7) U server sobi nije dozvoljeno fotografisanje, upotreba video i audio uređaja ili drugih uređaja za snimanje, izuzimajući osobe koje su za to pribavile pismeno odobrenje od direktora Sekretarijata odnosno rukovodioca pravosudne institucije.

*Član 33.*
*(Izvedba elektro i telekomunikacionih instalacija)*

Elektro i telekomunikacione instalacije u VSTV-u, odnosno pravosudnoj instituciji moraju biti izvedene na način da ih nije moguće nenamjerno prekinuti ili bez većih teškoća uništiti ili zloupotrijebiti.

*Član 34.*
*(Zaštita od požara)*

(1) Zaštita od požara u server sobi se vrši u skladu sa pozitivnim propisima o zaštiti od požara.

(2) U server sobi provode se sljedeće protivpožarne mjere:

a) zabrana pušenja;

b) zabrana upotrebe otvorenog plamena;

c) zabrana korištenja improvizovanih električnih uređaja i instalacija;

d) zabrana skladištenja zapaljivih materijala;

e) obavezno skladištenje nosača podataka (backup trake itd.) u zaključanim vatrootpornim ormarima.

(3) Server soba mora imati sistem za automatsku vatrodojavu povezan sa operativnim centrom organizacione jedinice nadležne za sigurnost VSTV-a, odnosno pravosudne institucije.

(4) Server soba mora biti opremljena sistemom za automatsko gašenje požara koji u slučaju aktiviranja ne smije biti štetan po zdravlje zaposlenih, te elektronsku, komunikacionu i IKT opremu i instalacije.

***Član 35.***
***(Politika "čistog stola")***

(1) Zaposleni ne smiju ostavljati nosače podataka sa osjetljivim sadržajem na otvorenim površinama kancelarijskog namještaja i opreme i drugim mjestima dostupnim neovlaštenim osobama. Svi nosači podataka s osjetljivim sadržajem moraju biti sklonjeni u vatrootporne ormare odnosno na drugi način zaštićeni.

(2) Zaposleni moraju da sprovode sljedeće mjere:

a) zaštititi prostorije i uređaje za prijem/otpremu pošte i faksova ako nisu posebno nadzirani;

b) osjetljive informacije odstraniti iz štampača ukoliko se štampaju.

(3) Po završetku radnog vremena obavezno je odjaviti se iz sistema i isključiti radnu stanicu, osim ako posebnim uputstvom nije izričito određeno drugačije.

***Član 36.***
***(Automatsko zaključavanje IKT opreme)***

(1) Radne stanice, serveri i ostala IKT oprema mora imati podešeno automatsko softversko zaključavanje koje onemogućava neovlašten pristup.

(2) Automatsko zaključavanje se mora samostalno aktivirati u slučaju neaktivnosti.

(3) Vremenski interval neaktivnosti propisan je posebnim uputstvom koji donosi šef Odjela za IKT.

***Član 37.***
***(Upravljanje otpadom)***

Prilikom uništavanja nosača podataka osjetljivog sadržaja onemogućava se čitanje svih dijelova uništenih podataka.

## POGLAVLJE IV - INFORMATIČKE MJERE SIGURNOSTI PRAVOSUDNOG INFORMACIONOG SISTEMA

### *Član 38.*
### *(Operativni postupci i odgovornosti)*

Sve informatičke mjere iz Politike sigurnosti su definisane kao minimalni standard za unapređenje sigurnosti pravosudnog informacionog sistema.

### *Član 39.*
### *(Dokumentovanje radnih postupaka)*

Radni postupci moraju biti formalno dokumentovani. Za potrebe upravljanja pravosudnim informacionim sistemom koriste se sljedeći dokumenti:

a) dokumentacija za upravljanje aplikativnim rješenjima i bazama podataka, uključujući uputstva;

b) mrežna i sistemska dokumentacija, uključujući uputstva;

c) dnevnici promjena;

d) dnevnici grešaka.

### *Član 40.*
### *(Razdvojenost produkcionog i testnog okruženja)*

(1) Pravosudni informacioni sistem čine tri međusobno razdvojena okruženja: produkciono, razvojno i testno.

(2) Direktor Sekretarijata odlukom utvrđuje koji servisi pravosudnog informacionog sistema moraju imati razvojno i testno okruženje.

(3) Okruženja su međusobno odvojena na nivou LAN mreže, servera i korisničkih prava pristupa.

(4) Razvojno i testno okruženje čine serveri namijenjeni razvoju i testiranju novih aplikacija. Za te servere vrijede iste sigurnosne mjere koje važe i za produkciono okruženje.

(5) Lični i drugi osjetljivi podaci iz produkcionog okruženja ne smiju biti pohranjeni u razvojnim i testnim bazama podataka.

(6) Prije prenosa hardverskog, mrežnog ili softverskog resursa iz razvojnog ili testnog u produkciono okruženje moraju biti provedene sve kontrolne tačke testiranja. Prenos se mora izvesti u skladu sa propisanim postupkom upravljanja promjenama iz ove Politike sigurnosti.

***Zaštita od zlonamjernih programa***

### *Član 41.*
### *(Zaštita od zlonamjernih programa)*

Na računarima i serverima pravosudnog informacionog sistema obavezna je zaštita od zlonamjernih programa.

*Član 42.*
*(Provjera ugroženosti datoteka na serverima i radnim stanicama)*

(1) Zaštita od zlonamjernih programa mora biti podešena na način da vrši provjeru ugroženosti datoteka u realnom vremenu.

(2) Najmanje jednom sedmično se vrši provjera sistemskih i korisničkih datoteka na serverima i radnim stanicama.

(3) Svi prenosni računari koji su dio pravosudnog informacionog sistema se moraju najmanje jednom mjesečno priključiti na LAN mrežu pravosudnog informacionog sistema i preuzeti najnovije nadogradnje softvera za zaštitu od zlonamjernih programa.

(4) Nije dozvoljeno onemogućavanje rada softvera za zaštitu od zlonamjernih programa.

*Član 43.*
*(Zaštita od zlonamjernih programa na ulazu u privatnu mrežu)*

Svi podaci primljeni preko protokola javne mreže moraju biti pregledani na postojanje zlonamjernih programa na ulazu u privatnu mrežu pravosudnog informacionog sistema.

*Član 44.*
*(Upravljanje softverom za zaštitu od zlonamjernih programa)*

(1) Softver za zaštitu od zlonamjernih programa mora biti instaliran tako da se za servere, radne stanice, prenosne računare i druge uređaje koji su trajno ili privremeno priključeni na LAN mreže pravosudnog informacionog sistema omogući centralno obavještavanje, evidentiranje događaja, statusa softvera i njegovih ažuriranja.

(2) Administriranje softvera za zaštitu od zlonamjernih programa vrše nadležni administratori Odjela za IKT.

(3) Provjera i ažuriranje softvera za zaštitu od zlonamjernih programa se mora vršiti automatski nakon što ažuriranja budu objavljena od strane proizvođača softvera.

*Član 45.*
*(Postupak provjere djelovanja zaštite od zlonamjernih programa)*

(1) Korisnik koji ustanovi da zaštita od zlonamjernih programa ne funkcioniše ili sumnja da se ona redovno ažurira mora o tome bez odlaganja obavijestiti nadležnog administratora.

(2) Nadležni administrator Odjela za IKT je dužan da redovno provjerava djelovanje zaštite od zlonamjernih programa i sistema za ažuriranje, a najmanje jednom sedmično djelovanje sistema za obavještavanje i evidentiranje događaja.

(3) Postupak u slučaju otkrivanja i uklanjanja zlonamjernih programa se detaljno propisuje uputstvom koje donosi šef Odjela za IKT.

*Član 46.*
*(Sigurnosne nadogradnje operativnog sistema na radnim stanicama i serverima pravosudnog informacionog sistema)*

(1) Sve radne stanice i serveri u pravosudnom informacionom sistemu moraju biti obuhvaćeni sistemom redovnih sigurnosnih nadogradnji operativnog sistema.

(2) Odjel za IKT dizajnira i implementira sistem iz stava (1) ovog člana. Šef Odjela za IKT donosi tehničko uputstvo kojim se detaljno propisuje opseg nadogradnje, vrijeme provođenja postupka nadogradnje i ostala vezana pitanja.

***Dokumentacija i dnevnici***

*Član 47.*
*(Upravljanje dokumentacijom pravosudnog informacionog sistema)*

Cjelokupna dokumentacija pravosudnog informacionog sistema mora da bude:

a) kreirana, pregledana i po potrebi revidirana najmanje jedanput godišnje ili nakon provođenja svake nadogradnje sistema;

b) potvrđena od strane šefa Odjela za IKT;

c) održavana na takav način da su jasno označene verzije i razlike među njima, te dostupna na svim lokacijama na kojima se provode aktivnosti od značaja za efikasno djelovanje;

d) dostupna u elektronskom obliku ovlaštenim administratorima određenim katalogom servisa iz člana 9. st. (1) i (2) Politike sigurnosti;

e) štampani primjerak aktuelne verzije dokumentacije sistema, zajedno sa svim parametrima, administrativnim i servisnim nalozima i šiframa, mora biti pohranjen u vatrootpornom sefu Odjela za IKT odnosno sefu pravosudne institucije.

*Član 48.*
*(Sistemska dokumentacija)*

(1) Odjel za IKT, odnosno IKT službenik obezbjeđuje izradu i ažuriranje sistemske dokumentacije, njenu raspoloživost i zaštitu, za resurse pravosudnog informacionog sistema za koje je nadležan.

(2) O sistemskoj dokumentaciji svakog pojedinačnog resursa pravosudnog informacionog sistema se brine nadležni administrator resursa.

*Član 49.*
*(Pregled i zaštita dnevnika)*

(1) Nadzor nad pravosudnim informacionim sistemom i pravilnost funkcionisanje kontroliše se putem sistema za nadzor i upravljanje svakog resursa. U njima se čuvaju sadržaji dnevničkih zapisa.

(2) Dnevničke zapise mora redovno pregledati nadležni administrator tog resursa.

(3) Uočeni kritični događaji se upisuju u dnevnik grešaka koji sadrži: vrijeme nastanka greške odnosno sigurnosnog incidenta, vrstu kritičnog događaja, zapažanje o uticaju na djelovanje sistema, uzrok (ako je poznat), način otklanjanja greške, vrijeme otklanjanja greške, zaduženu osobu.

(4) Dnevnički zapisi se moraju zaštitno kopirati u skladu sa posebnim tehničkim uputstvom koje će urediti proceduru upravljanja i rokove čuvanja dnevničkih zapisa, a koje donosi šef Odjela za IKT.

(5) Dnevnički zapisi se ne smiju ručno brisati.

***Izrada rezervnih kopija sistema i podataka***

***Član 50.***
***(Rezervne kopije resursa i podataka)***

(1) Ključni resursi i podaci u pravosudnom informacionom sistemu moraju biti obuhvaćeni procesom izrade rezervnih kopija (u daljem tekstu backup).

(2) Posebnim tehničkim uputstvom koje donosi šef Odjela za IKT se definiše način i dinamika izrade backupa za svaki pojedinačni resurs.

(3) Nadležni administrator Odjela za IKT zadužen je za izradu backupa sistema i podataka na serverima u data centrima pravosudnog informacionog sistema.

(4) IKT službenik je zadužen za izradu backupa sistema i podataka na serverima za koje je nadležan, uključujući individualne direktorije korisnika i zajednički direktorij institucije.

(5) Korisnici su dužni da sve datoteke, čiji bi eventualni gubitak mogao proizvesti poteškoće u obavljanju poslova njihovog radnog mjesta, pohranjuju na file serveru pravosudne institucije kojoj pripadaju.

***Član 51.***
***(Čuvanje backupa podataka)***

(1) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije, vodeći računa o finansijskim i tehnološkim mogućnostima, donosi odluku o obaveznom načinu čuvanja backupa podataka, bilo da se oni čuvaju samostalno ili kod vanjskog pružaoca usluge.

(2) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije određuje vanjske lokacije na kojima se čuvaju backupi iz stava (1) ovog člana.

***Nosači podataka***

***Član 52.***
***(Čuvanje i zaštita prenosnih nosača podataka)***

(1) Korisnici ne smiju čuvati povjerljive dokumente, dokumente od kritične važnosti za rad institucije ili dokumente koji sadrže lične podatke na nezaštićenim prenosnim nosačima podataka.

(2) Zaštita nosača podataka iz stava (1) ovog člana se vrši prema tehničkom uputstvu koje donosi šef Odjela za IKT.

(3) Nosače podataka iz stava (1) ovog člana mogu da iznose iz prostorija VSTV-a odnosno pravosudne institucije samo za to ovlaštene osobe. Listu ovlaštenih osoba donosi nadležni rukovodeći državni službenik u VSTV-u odnosno rukovodilac pravosudne institucije.

(4) Sve ovlaštene osobe iz stava (3) ovog člana su dužne potpisati izjavu o prihvatanju odgovornosti u slučaju gubitka nosača podataka iz stava (1) ovog člana.

(5) U slučaju nestanka ili krađe nosača podataka iz stava (1) ovog člana, potrebno je obavijestiti direktora Sekretarijata odnosno rukovodioca pravosudne institucije koji će po potrebi naložiti provođenje odgovarajućih postupaka.

(6) Sa nosačima podataka nepoznatog izvora se postupa u skladu sa tehničkim uputstvom koje donosi šef Odjela za IKT.

***Član 53.***
***(Postupanje sa nosačima podataka koji se izdvajaju)***

(1) Sa nosača podataka predviđenih za izdvajanje moraju se na siguran način uništiti podaci. Uništenje podataka mora biti izvedeno tako da ih nije moguće obnoviti u cjelini ili djelimično.

(2) U tu svrhu primjenjuju se postupci propisani posebnim tehničkim uputstvom koje donosi šef Odjela za IKT.

(3) Ukoliko je to potrebno i moguće, podaci se prije brisanja prenose u drugi sistem odnosno na druge nosače.

(4) Odredbe stava (1) ovog člana se ne primjenjuju na neispravne i neupotrebljive nosače podataka, koji se u skladu sa uslovima garancije moraju vratiti proizvođaču kako bi se zamijenili novim.

(5) Ukoliko direktor Sekretarijata, odnosno rukovodilac pravosudne institucije na prijedlog šefa Odjela za IKT, odnosno IKT službenika ocijeni da nosač podataka iz stava (4) ovog člana sadrži podatke povjerljive prirode, donosi odluku o njegovom izdvajanju i postupanju na način predviđen stavom (1) ovog člana.

(6) Ako uništavanje nosača vrši vanjski saradnik, ono mora biti izvršeno pod nadzorom ovlaštene osobe VSTV-a, odnosno pravosudne institucije.

(7) Cjelokupan postupak uništenja, u skladu sa ovim članom, se zapisnički konstatuje.

***Korisnički nalozi i šifre***

***Član 54.***
***(Korisnički nalozi i šifre)***

(1) Za svaki korisnički nalog odgovorna je samo jedna osoba. Jedna osoba može imati više korisničkih naloga.

(2) Svaki korisnički nalog mora biti zaštićen šifrom, koja ne smije biti otkrivena drugima.

(3) Šifra ne smije biti kreirana na osnovu ličnih podataka, imena članova porodice, kućnih ljubimaca, geografskih i sličnih pojmova, uobičajenih riječi i sl.

(4) Šifra ne smije biti zapisana ili čuvana na mjestu lako dostupnom drugima.

(5) Šef Odjela za IKT donosi posebno tehničko uputstvo kojim se uređuju pravila za kreiranje i upravljanje korisničkim nalozima i šiframa.

*Član 55.*
***(Administrativni i servisni nalozi i šifre resursa pravosudnog informacionog sistema)***

(1) Svaki administrativni i servisni nalog mora biti zaštićen šifrom.

(2) Šifra ne smije biti kreirana na osnovu ličnih podataka, imena članova porodice, kućnih ljubimaca, geografskih i sličnih pojmova, uobičajenih riječi i sl.

(3) Šifra ne smije biti zapisana ili čuvana na mjestu lako dostupnom drugima.

(4) Za generičke administrativne i servisne naloge moraju biti imenovani nadležni administratori.

(5) Svaka šifra poznata administratoru Odjela za IKT, odnosno IKT službeniku obavezno se mijenja u slučaju prestanka njegovog radnog odnosa u VSTV-u, odnosno pravosudnoj instituciji.

(6) Šef Odjela za IKT donosi posebno tehničko uputstvo kojim se uređuju pravila za kreiranje i upravljanje administrativnim i servisnim nalozima i šiframa.

*Član 56.*
***(Deponovanje administrativnih i servisnih naloga i šifri)***

Administrativni i servisni nalozi i šifre se moraju sigurno deponovati za slučaj:

a) vanrednih događaja;

b) da nadležni administrator šifru zaboravi;

c) da nadležni administrator nije prisutan, a neophodno je obaviti intervenciju na resursu, za što je potrebna šifra.

*Član 57.*
***(Odgovornost za deponovanje administrativnih i servisnih naloga i šifri)***

(1) Šef Odjela za IKT je dužan uspostaviti popis resursa u nadležnosti Odjela za IKT u/na kojima se koriste administrativni i servisni nalozi i šifre i da se stara o tome da se nadležni administratori pridržavaju pravila njihovog deponovanja.

(2) Rukovodilac pravosudne institucije je dužan uspostaviti popis resursa u nadležnosti pravosudne institucije u/na kojima se koriste administrativni i servisni nalozi i šifre i da se stara o tome da se nadležni administratori pridržavaju pravila njihovog deponovanja.

(3) Administrativni i servisni nalozi i šifre se zapisuju i čuvaju u posebnim kovertama, koje moraju biti zapečaćene. Na koverti se obavezno ispisuje:

a) oznaka "ZABRANJENO OTVARANJE NEOVLAŠTENIM LICIMA";

b) naziv institucije;

c) naziv resursa na koji se primjenjuje šifra.

(4) Podaci koji su pohranjeni unutar koverte su definisani na posebnom obrascu koji donosi šef Odjela za IKT.

(5) Zapečaćene koverte deponuju nadležni administratori odnosno osobe koje se staraju o pojedinim resursima pravosudnog informacionog sistema.

(6) Zapečaćene koverte se čuvaju u vatrootpornom sefu u kontrolisanom prostoru unutar VSTV-a, odnosno pravosudne institucije ili na vanjskoj lokaciji (npr. u iznajmljenom sefu u banci).

***Član 58.***
***(Pristup zapečaćenim kovertama sa administrativnim i servisnim nalozima i šiframa)***

(1) Pristup sefu u kojem su deponovani administrativni i servisni nalozi i šifre dozvoljen je samo uz odobrenje šefa Odjela za IKT odnosno rukovodioca pravosudne institucije ili od njih ovlaštenih osoba.

(2) Pristup sefu iz stava (1) ovog člana evidentira se u posebnom dnevniku, koji sadrži sljedeće podatke: datum i vrijeme pristupanja, resurs, ime i prezime osobe koja vrši pristup i osobe koja daje odobrenje, razlog pristupa i njihov potpis.

***Član 59.***
***(Promjena šifre nakon otvaranja zapečaćenih koverti sa administrativnim i servisnim nalozima i šiframa)***

(1) Nakon promjene šifre administrativnog ili servisnog naloga, ista se ponovo deponuje na način opisan u članu 57. Politike sigurnosti.

(2) Nakon promjene šifre iz stava (1) ovog člana, koverta sa starom šifrom se fizički uništava, uključujući i šifru deponovanu na vanjskoj lokaciji.

***Računarske mreže***

***Član 60.***
***(Korištenje i sigurnost mrežnih usluga)***

(1) Mreža pravosudnog informacionog sistema omogućava nesmetanu komunikaciju korisnika i odobrenih servisa.

(2) Upotreba mreže suprotno stavu (1) ovog člana je zabranjena i tretira se kao incident iz oblasti sigurnosti pravosudnog informacionog sistema.

***Član 61.***
***(Upravljanje mrežama pravosudnog informacionog sistema)***

(1) Odjel za IKT osigurava tehničku zaštitu od neovlaštenog upada između pravosudne WAN mreže i Internet mreže ili bilo koje druge forme vanjske mreže.

(2) Sva priključenja uređaja koji nisu vlasništvo VSTV-a na LAN mrežu u data centrima i prostorijama VSTV-a moraju biti odobrena od strane šefa Odjela za IKT i pravovremeno najavljena nadležnom administratoru Odjela za IKT, koji provodi sve tehničke radnje potrebne za navedeno priključenje.

(3) Sva priključenja na LAN mrežu pravosudnih institucija moraju biti odobrena od strane sudske/tužilačke uprave i pravovremeno najavljena IKT službeniku pravosudne institucije, koji provodi sve tehničke radnje potrebne za navedeno priključenje.

(4) Sva priključenja računara koji su u vlasništvu pravosudnih institucija, ali nisu dio pravosudnog informacionog sistema, na LAN mrežu pravosudnih institucija, moraju biti odobrena od strane šefa Odjela za IKT.

(5) Mobilnim uređajima i prenosnim računarima posjetilaca dozvoljeno je samo povezivanje na posebne mrežne segmente namijenjene pristupu Internetu, ukoliko isti postoje.

(6) Prije nego što se odobri pristup mrežnim resursima, sva oprema iz stava (5) ovog člana se mora autentifikovati.

(7) Način i tehnike zaštite mreža pravosudnog informacionog sistema se utvrđuju posebnim tehničkim uputstvom koje donosi šef Odjela za IKT.

***Član 62.***
***(Vanjski pristup mrežama pravosudnog informacionog sistema)***

(1) Za pristup pojedinim servisima odnosno resursima u LAN mrežama pravosudnog informacionog sistema preko Interneta koriste se kriptovane veze VPN tehnologije.

(2) Upravljanje i nadzor nad vanjskim pristupom iz stava (1) ovog člana vrši nadležni administrator Odjela za IKT.

(3) Vanjski pristup iz stava (1) ovog člana odobrava šef Odjela za IKT.

(4) Način i tehnike korištenja VPN tehnologije se utvrđuju posebnim tehničkim uputstvom koje donosi šef Odjela za IKT.

(5) Odjel za IKT će elektronski evidentirati i kontrolisati pristup ovlaštenih korisnika van pravosudnog informacionog sistema prema pravosudnoj WAN mreži koja se ostvaruje putem VPN tehnologije.

***Član 63.***
***(Odvajanje mreža)***

(1) LAN mreža u data centru i prostorijama VSTV-a se mora odvojiti u logičke segmente kako bi se na taj način osigurala kontrola pristupa serverima i drugim uređajima koji pripadaju određenom logičkom segmentu.

(2) Konfigurisanje logičkih segmenata izvodi se u skladu sa tehničkim uputstvom koje donosi šef Odjela za IKT.

(3) Zahtjev za promjenu konfiguracije parametara mreže iz stava (1) ovog člana, te pravosudne WAN mreže upućuje se šefu Odjela za IKT.

(4) Promjene iz stava (3) ovog člana vrši nadležni administrator Odjela za IKT.

***Elektronska pošta i Internet***

***Član 64.***
***(Prihvatljiva upotreba elektronske pošte)***

Elektronska pošta pravosudnog informacionog sistema (u daljem tekstu: elektronska pošta) koristi se u službene svrhe.

***Član 65.***
***(Neprihvatljiva upotreba elektronske pošte)***

Neprihvatljivu upotrebu elektronske pošte predstavlja:

a) korištenje elektronske pošte u suprotnosti sa važećim zakonskim propisima posebno na način koji predstavlja krivično djelo ili prekršaj;

b) korištenje elektronske pošte na način da se onemogućava normalno funkcionisanje sistema elektronske pošte, pravosudnog informacionog sistema ili ometa rad drugih korisnika;

c) korištenje elektronske pošte u svrhu sticanja profita, lične dobiti ili obavljanje javnih aktivnosti koji nisu u vezi sa poslovima radnog mjesta;

d) distribucija komercijalnih i marketinških poruka;

e) slanje materijala kojim se krše autorska prava;

f) slanje izvršnih datoteka putem elektronske pošte;

g) namjerno propagiranje zlonamjernih programa;

h) slanje materijala neprimjerenog, uvredljivog ili opscenog sadržaja, te materijala koji poziva na mržnju i netoleranciju;

i) slanje bilo kojeg sadržaja koji se smatra uznemirujućim;

j) slanje ličnih podataka bez saglasnosti nosioca ličnih podataka;

k) lažno predstavljanje korisnika elektronske pošte i institucije u porukama elektronske pošte.

***Član 66.***
***(Postupak u slučaju uočavanja neprihvatljive upotrebe elektronske pošte)***

(1) Dužnost je svakog korisnika elektronske pošte ili nadležnog administratora koji uoči neprihvatljivu upotrebu elektronske pošte da o tome obavijesti Odjel za IKT.

(2) Odjel za IKT će o ovome informisati relevantnog rukovodećeg državnog službenika u VSTV-u odnosno rukovodioca pravosudne institucije kojoj pripada korisnik koji je izvršio radnju koja predstavlja neprihvatljivu upotrebu elektronske pošte.

(3) Korisnik koji na neprihvatljiv način upotrebljava elektronsku poštu biće upozoren od strane relevantnog rukovodećeg državnog službenika u VSTV-u odnosno rukovodioca pravosudne institucije.

(4) U slučaju ponovljene neprihvatljive upotrebe elektronske pošte od strane istog korisnika, odjel za IKT će prema takvom korisniku odmah primijeniti privremenu mjeru zabrane slanja elektronske pošte i o istome obavijestiti relevantnog rukovodećeg državnog službenika u VSTV-u odnosno rukovodioca pravosudne institucije kojoj korisnik pripada.

(5) Zahtjev za ukidanje privremene mjere zabrane slanja elektronske pošte relevantni rukovodeći državni službenik odnosno rukovodilac pravosudne institucije upućuje Odjelu za IKT pismenim putem. Odjel za IKT će razmotriti zahtjev i obavijestiti relevantnog rukovodećeg državnog službenika u VSTV-u odnosno rukovodioca pravosudne institucije o statusu privremene zabrane slanja elektronske pošte.

*Član 67.*
*(Zaštita sistema elektronske pošte)*

(1) Korisnici su dužni da sve poruke i priloge u porukama sumnjivog sadržaja, te upozorenja o mogućoj sigurnosnoj prijetnji pravosudnom informacionom sistemu, odmah prijave IKT službeniku institucije kojoj pripadaju ili Odjelu za IKT u slučaju odsustva IKT službenika, ne otvarajući iste.

(2) IKT službenik je dužan da sve zaprimljene prijave iz stava (1) ovog člana odmah proslijedi Odjelu za IKT.

(3) Odjel za IKT će pažljivo istražiti svako upozorenje i preduzeti odgovarajuće mjere.

(4) Korisnicima elektronske pošte nije dozvoljeno da samostalno šalju upozorenja drugim korisnicima o mogućoj sigurnosnoj prijetnji pravosudnom informacionom sistemu.

*Član 68.*
*(Pristup elektronskoj pošti)*

(1) Svi korisnici pravosudnog informacionog sistema ostvaruju pristup sistemu elektronske pošte putem softverske aplikacije odobrene od strane Odjela za IKT iz LAN mreža pravosudnih institucija.

(2) Pristup sistemu elektronske pošte izvan pravosudne WAN mreže, a putem Interneta ostvaruju samo korisnici koji su odlukom rukovodioca institucija ovlašteni za ostvarivanje ovog pristupa.

*Član 69.*
*(Pristup Internetu)*

(1) Odjel za IKT je zadužen za kreiranje funkcionalnog i sigurnog pristupa Internetu korisnika pravosudnog informacionog sistema.

(2) Pravo pristupa Internetu ostvaruju ovlašteni korisnici u pravosudnim institucijama.

(3) Odjel za IKT zadržava pravo da ograniči ukupan broj korisnika koji ostvaruju pristup Internetu ukoliko to zahtijevaju finansijski ili tehnički razlozi.

(4) Kada nastupe okolnosti iz stava (3) ovog člana, rukovodioci pravosudnih institucija su dužni dostaviti na zahtjev Odjela za IKT listu korisnika koji će ostvarivati pristup Internetu čiji broj ne smije prelaziti broj određen od strane Odjela za IKT.

(5) Pristup Internetu se vrši putem pravosudne WAN mreže i pristupnih tački u data centrima VSTV-a.

*Član 70.*
*(Prihvatljiva upotreba Interneta)*

Pristup Internetu je omogućen u poslovne svrhe.

*Član 71.*
*(Neprihvatljiva upotreba Interneta)*

(1) Neprihvatljiva upotreba Interneta podrazumijeva:

a) korištenje Interneta u suprotnosti sa važećim zakonskim propisima posebno na način koji predstavlja krivično djelo ili prekršaj;

b) kršenje autorskih prava preuzimanjem i instaliranjem neautorizovanog softvera i korištenjem neautorizovanih elektronskih dokumenata;

c) neovlašteno preuzimanje softvera, izvršnih datoteka, baza podataka i sličnih elektronskih dokumenata na radne stanice pravosudnog informacionog sistema;

d) narušavanje integriteta pravosudnog informacionog sistema namjernim propagiranjem zlonamjernih programa, zagušivanjem Internet saobraćaja, pokušajem zaobilaženja mjera sigurnosti i dodijeljenih prava pristupa i sličnim radnjama;

e) korištenje Interneta u svrhu sticanja profita, lične dobiti ili obavljanje javnih aktivnosti koje nisu u vezi sa poslovima radnog mjesta;

f) pregledavanje web stranica neprimjerenog, uvredljivog, zastrašujućeg ili opscenog sadržaja;

g) upražnjavanje igara i klađenja;

h) lažno predstavljanje korisnika i institucije na Internetu;

i) neovlašteno korištenje chat grupa i socijalnih mreža;

j) neovlašteno korištenje video i audio streaminga;

k) dijeljenje datoteka sa osobama i subjektima izvan pravosudnog informacionog sistema;

l) korištenje Internet i drugih javnih ili privatnih usluga za čuvanje i razmjenu podataka;

m) prenošenje i objavljivanje povjerljivih informacija, neovlašteno popunjavanje elektronskih anketa usmjerenih na davanje podataka povjerljive ili interne prirode.

(2) Odjel za IKT provodi tehničke mjere uvođenja ograničenja pristupa Internetu isključivo u cilju suzbijanja neprihvatljive upotrebe Interneta iz stava (1) ovog člana putem za to specijalizovanog hardvera i softvera.

***Član 72.***
***(Postupak u slučaju uočavanja neprihvatljive upotrebe Interneta)***

(1) Odjel za IKT će odmah, kada to uoči, obavijestiti relevantnog rukovodećeg državnog službenika u VSTV-u, odnosno rukovodioca pravosudne institucije kojoj pripada korisnik koji je izvršio radnju koja predstavlja neprihvatljivu upotrebu Interneta.

(2) Korisnik koji na neprihvatljiv način upotrebljava Internet biće upozoren od strane relevantnog rukovodećeg državnog službenika u VSTV-u odnosno rukovodioca pravosudne institucije.

(3) U slučaju ponovljene neprihvatljive upotrebe Interneta od strane istog korisnika, Odjel za IKT će prema takvom korisniku odmah primijeniti privremenu mjeru zabrane pristupa Internetu i o tome obavijestiti relevantnog rukovodećeg državnog službenika u VSTV-u odnosno rukovodioca pravosudne institucije kojoj korisnik pripada.

(4) Pismeni zahtjev za ukidanje privremene mjere zabrane pristupa Internetu relevantni rukovodeći državni službenik odnosno rukovodilac pravosudne institucije upućuje Odjelu za IKT, koji će razmotriti zahtjev i obavijestiti relevantnog rukovodećeg državnog službenika u VSTV-u, odnosno rukovodioca pravosudne institucije o statusu privremene zabrane pristupa Internetu.

*Član 73.*
*(Praćenje Internet saobraćaja)*

Odjel za IKT vrši elektronsko evidentiranje Internet stranica kojima pristupaju pojedinačni korisnici u svrhu upravljanja mrežama i sigurnošću pravosudnog informacionog sistema.

***Prenosna oprema***

*Član 74.*
*(Fizička i softverska zaštita prenosne opreme)*

(1) Korisnici prenosne opreme u vlasništvu VSTV-a odnosno pravosudne institucije su dužni preduzeti sve potrebne radnje da bi istu zaštitili od otuđenja i/ili neovlaštenog pristupa.

(2) Odjel za IKT donosi preporuke za postupanje sa prenosnom opremom u svrhu minimiziranja rizika za njeno otuđenje i/ili neovlašteni pristup.

(3) Obavezna je enkripcija podataka na prenosnim računarima.

(4) Šef Odjela za IKT donosi tehničko uputstvo kojim se propisuju minimalni standardi softverske zaštite prenosnih uređaja i u njima pohranjenih podataka.

*Član 75.*
*(Zaštita pametnih mobilnih aparata)*

U svrhu zaštite pametnih mobilnih aparata primjenjuju se sljedeća pravila:

a) pristup mobilnom aparatu mora biti zaštićen šifrom prema tehničkom uputstvu koje donosi šef Odjela za IKT;

b) automatsko zaključavanje se mora samostalno aktivirati u slučaju neaktivnosti korisnika;

c) za slučaj krađe ili nestanka mobilnog aparata, zaključani ekran uređaja mora prikazivati kontakt informacije korisnika (ime i prezime, naziv institucije, adresu elektronske pošte i službeni fiksni telefonski broj).

*Član 76.*
*(Ostala pravila za prenosnu opremu)*

Korisnik koji na privatnom prenosnom uređaju koristi servise pravosudnog informacionog sistema je dužan iste koristiti u skladu sa zahtjevima i prema ograničenjima koja propisuje Politika sigurnosti, o čemu potpisuje posebnu izjavu.

***Postupci u slučaju vanrednog događaja***

*Član 77.*
*(Mogući vanredni događaji)*

(1) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije utvrđuje osnovne elemente kriznog upravljanja s ciljem nastavka poslovnih procesa u ograničenom odnosno punom obimu u slučaju vanrednih događaja.

(2) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije osigurava provođenje procjene ugroženosti s prijedlogom mjera za njihovo smanjenje ili otklanjanje.

(3) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije utvrđuje glavne moguće vanredne događaje i procjenjuje vjerovatnoću da do njih dođe.

***Član 78.***
***(Ključni poslovni procesi i zadaci)***

(1) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije osigurava utvrđivanje ključnih procesa/zadataka i razvrstava ih po značaju.

(2) U slučaju vanrednog događaja poštuje se klasifikacija poslovnih procesa/zadataka iz stava (1) ovog člana i u skladu s njom izvršava akcioni plan za uspostavljanje funkcionalnog, a kasnije i normalnog stanja (vraćanje u prvobitno stanje).

(3) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije upravlja mjerama i aktivnostima u slučaju vanrednog događaja u skladu sa akcionim planom iz stava (2) ovog člana.

(4) Plan iz stava (2) ovog člana mora biti dokumentovan i ažuran.

***Član 79.***
***(Podaci za ključne kontakte)***

(1) Odjel za AKP, odnosno sudska/tužilačka uprava izrađuje i ažurira popis ovlaštenih lica, ključnih dobavljača, telefonskih brojeva interventnih službi (vatrogasci, hitna pomoć, policija, sudska policija, službe osiguranja) i drugih podataka potrebnih za realizaciju planova i mjera u slučaju vanrednog događaja.

(2) Odjel za IKT, odnosno IKT službenik izrađuje i ažurira popis dobavljača odnosno pružaoca usluga održavanja resursa pravosudnog informacionog sistema, njihovih kontakt podataka i drugih podataka potrebnih za realizaciju planova i mjera u slučaju vanrednog događaja.

***Član 80.***
***(Komunikacija)***

(1) Planovi i mjere u slučaju vanrednog događaja u VSTV-u, odnosno pravosudnoj instituciji se izvršavaju internim osposobljavanjem zaposlenih, održavanjem internih sastanaka i, najmanje jednom godišnje, simuliranjem vanrednog događaja.

(2) U slučaju izbijanja vanrednog događaja sa zaposlenima, poslovnim partnerima i javnošću se kontaktira usmeno ili elektronskom poštom ukoliko je to moguće.

***Član 81.***
***(Zaštitne kopije ključne dokumentarne građe)***

(1) Direktor Sekretarijata, odnosno rukovodilac pravosudne institucije imenuje osobu odgovornu za zaštitne kopije ključnih dokumenata i zapisa VSTV-a, odnosno pravosudne institucije.

(2) Zaštitne kopije dokumenata, planovi, finansijski podaci, police osiguranja, bankovni računi, sistemski backupi i drugi dokumenti od ključnog značaja za poslovanje VSTV-a, odnosno pravosudne institucije, posebno se osiguravaju i čuvaju.

(3) Ako su ključni dokumenti i zapisi u slučaju vanrednog događaja uništeni, direktor Sekretarijata, odnosno rukovodilac pravosudne institucije organizuje nastavak poslovanja rekonstrukcijom podataka iz zaštitnih kopija.

***Član 82.***
***(Plan oporavka)***

(1) Odjel za IKT odnosno IKT službenik izrađuje plan oporavka (engl. disaster recovery plan) ključnih servisa pravosudnog informacionog sistema za koje je nadležan, u kojem se navodi vrijeme potrebno za oporavak, detaljni koraci postupka oporavka servisa, te nadležne osobe za svaki pojedinačni korak.

(2) Ključni servisi su određeni akcionim planom iz člana 78. stav (2) Politike sigurnosti.

(3) Plan oporavka se ažurira nakon svake promjene na resursima.

(4) Plan oporavka se provjerava najmanje jedanput godišnje.

(5) Ukoliko se u postupku iz stava (4) ovog člana ustanove odstupanja većeg obima, provode se aktivnosti koje će unaprijediti oporavak.

(6) Svi postupci provjere se dokumentuju, a o rezultatima se izvještava direktor Sekretarijata odnosno rukovodilac pravosudne institucije.

## POGLAVLJE: PRELAZNE I ZAVRŠNE ODREDBE

***Član 83.***
***(Kršenje odredbi Politike sigurnosti)***

(1) U slučaju kršenja odredbi Politike sigurnosti prekršiocu se može izreći mjera zabrane korištenja određenog servisa pravosudnog informacionog sistema.

(2) Prema korisniku koji prekrši pravila Politike sigurnosti postupit će se u skladu sa propisima koji se primjenjuju na njegovu disciplinsku odgovornost.

(3) Vanjski saradnici koji se ne pridržavaju odredbi Politike sigurnosti gube pravo saradnje sa VSTV-om, odnosno pravosudnim institucijama. U slučaju težih kršenja odredbi Politike sigurnosti može se protiv takvih pravnih ili fizičkih lica pokrenuti odštetni ili drugi postupak pred nadležnim organima.

***Član 84.***
***(Uputstva za primjenu)***

Uputstva i drugi akti potrebni za provođenje Politike sigurnosti donijet će se u roku od devet mjeseci od dana donošenja Politike sigurnosti.

***Član 85.***
***(Stupanje na snagu)***

Politika sigurnosti stupa na snagu nakon šest mjeseci od dana donošenja.

Broj: 09-29-1-3231/2016
Sarajevo, 10.11.2016. godine

MP

Predsjednik
Milan Tegeltija