BOSNA I HERCEGOVINA
REPUBLIKA SRPSKA
OSNOVNI SUD U ZVORNIKU
BROJ: 083-0-SU-21-001 263
Datum, 30.12.2021. godine

Na osnovu člana 48. Zakona o sudovima Republike Srpske („Službeni glasnik Republike Srpske", broj: 37/12, 44/15 i 100/17) i člana 8. stav 1. tačka r) Pravilnika o unutrašnjem sudskom poslovanju („Službeni glasnik Republike Srpske", broj: 9/14, 71/17, 67/18 i 6/19) predsjednik suda, d o n o s i

POLITIKU SIGURNOSTI INFORMACIONOG SISTEMA OSNOVNOG SUDA U ZVORNIKU

SADRŽAJ

POGLAVLJE I – OPŠTE ODREDBE

Član 1.
(Predmet)

Politikom sigurnosti informacionog sistema Osnovnog suda u Zvorniku (u daljem tekstu: Politika sigurnosti) se:

a) uređuje upravljanje sigurnošću informacionog sistema Osnovnog suda u Zvorniku (u daljem tekstu informacioni sistem);

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

Član 2.
(Svrha)

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

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

b) da 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 informacionog sistema Osnovnog suda u Zvorniku i u njima pohranjenim informacijama, njihovog uništavanja, otuđenja ili otkrivanja neovlaštenim licima;

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

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

d) podizanje nivoa svijesti i odgovornosti zaposlenih u Osnovnom sudu u Zvorniku 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) osiguravanje usklađenosti korištenja informacionog sistema sa pozitivnim propisima u Bosni i Hercegovini i relevantnim standardima.

Član 4.
(Obim primjene)

Politika sigurnosti informacionog sistema se primjenjuje na:

a) sudije i sve zaposlene u Osnovnom sudu u Zvorniku;

b) zgrade Osnovnog suda u Zvorniku;

c) lokalnu računarsku mrežu (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 informacionog sistema, zaštita na radu, sigurnost finansijskih transakcija i drugo, čija zloupotreba može ugroziti sigurnost informacionog sistema.

Član 5.
(Odgovornost za primjenu)

(1) Predsjednik suda preduzima organizacione mjere, te obezbjeđuju finansijske, kadrovske i druge resurse i sredstva potrebna za funkcionisanje informacionog sistema u skladu sa svojim ovlaštenjima i odredbama Politike sigurnosti.

(2) Službenik za informaciono-komunikacionu tehnologiju u Osnovnom sudu u Zvorniku (u daljem tekstu: IKT službenik) je zadužen za provođenje tehničkih mjera za funkcionisanje informacionog sistema u skladu sa odredbama Politike sigurnosti.

(3) IKT službenik provodi mjere predviđene Politikom sigurnosti iz člana 12. Politike sigurnosti.

(4) Svi zaposleni u sudu obavezni su pridržavati se odredbi Politike sigurnosti.

(5) Svi zaposleni u sudu dužni su da s najvišim stepenom pažnje postupaju sa podacima, informacijama i resursima 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 Osnovnog suda u Zvorniku koji se koristi za obavljanje poslova i zadataka iz nadležnosti Osnovnog suda u Zvorniku.

(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 Osnovnog suda u Zvorniku koji je obuhvaćen mjerama pojačane fizičke i tehničke zaštite.

(17) Data centar informacionog sistema je server soba Osnovnog suda u Zvorniku u kojoj su smješteni ključni resursi 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 VSTS-u i pravosudnim institucijama u Bosni i Hercegovini. Pravosudni informacioni sistem obuhvata sve sisteme čije korištenje vodi, koordinira i nadgleda VSTS.

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

(32) Dnevnik ulazaka je evidencija svih pristupa server sobi Osnovnog suda u Zvorniku.

(33) IKT službenik je zaposleno lice kod Osnovnog suda u Zvorniku koji u okviru poslova u pravosudnoj instituciji vrši nadzor, održavanje, upravljanje i administriranje dijela pravosudnog informacionog sistema u Osnovnom sudu u Zvorniku u okviru svojih nadležnosti. IKT službenik ima ulogu administratora u Osnovnom sudu u Zvorniku.

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

(35) 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.

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

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

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

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

(40) 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.

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

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

(43) Odjel za IKT je Odjel za informaciono-komunikacionu tehnologiju pri Sekretarijatu VSTS-a BiH.

POGLAVLJE II – INFORMACIONI SISTEM

Član 7.
(Katalog servisa)

(1) Predsjednik suda odlukom utvrđuje katalog servisa informacionog sistema koji su u nadležnosti Osnovnog suda u Zvorniku, te određuje poslovni značaj i odgovorne osobe za upravljanje svakim pojedinačnim servisom.

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

Član 8.
(Korisnici informacionog sistema)

Korisnici informacionog sistema su sudije i drugi zaposleni u Osnovnom sudu u Zvorniku, te fizička i pravna lica koja koriste servise informacionog sistema.

Član 9.
(Razvoj informacionog sistema)

(1) Razvoj 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) U pogledu strateške politike razvoja informacionog sistema Osnovni sud u Zvorniku postupa u skladu sa odredbama člana 11. Politike sigurnosti pravosudnog informacionog sistema BiH

(3) Predsjednik suda je dužan osigurati organizacione i kadrovske preduslove za nesmetano provođenje projekata razvoja pravosudnog informacionog sistema koje odobri VSTS, od faze planiranja do faze implementacije u Osnovnom sudu u Zvorniku u skladu sa članom 11. Politike sigurnosti pravosudnog informacionog sistema BiH.

Član 10.
(Principi upravljanja promjenama u informacionom sistemu)

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

a) promjene moraju biti odobrene od strane IKT službenika;

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 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.

Član 11.
(Administriranje i održavanje informacionog sistema)

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

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

Član 12.
(Administriranje resursa informacionog sistema)

(1) IKT službenik u Osnovnom sudu u Zvorniku administrira:

a) korisničke naloge za sudije 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 VSTS-a, ukoliko je posebnim propisima ili odlukama njihovo administiranje povjereno IKT službenicima;

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

Član 13.
(Redovni nadzor informacionog sistema)

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

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

Član 14.
(Vanredni nadzor informacionog sistema)

(1) Vanredni nadzor podrazumijeva elektronski uvid u korisničke podatke kreirane, poslane, primljene i pohranjene u informacionom sistemu i vrši se po pismenom nalogu predsjednika suda ili ovlaštenog radnika suda koga za to pismenim putem ovlasti predsjednik suda.

(2) Vanredni nadzor vrši IKT službenik u sljedećim situacijama:

a) istraga o navodima kršenja zakona od strane korisnika;

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

c) istraga o narušavanju sigurnosti 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 15.
(Postupanje u slučaju incidenata iz oblasti sigurnosti informacionog sistema)

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

(2) Svaki korisnik koji uoči incident u smislu Politike sigurnosti je dužan bez odlaganja obavijestiti IKT službenika i dostaviti mu sve relevatne informacije vezane za incident.

(3) IKT službenik analizira dostavljene informacije i podnosi izvještaj predsjedniku suda. Izvještaj sadrži i prijedlog mjera koje je potrebno preduzeti u cilju rješavanja incidenta.

(4) Na osnovu izvještaja predsjednik suda može IKT službeniku uputiti nalog za vanredni nadzor iz člana 14. stav 1. Politike sigurnosti ili naložiti preduzimanje drugih tehničkih mjera.

(5) IKT službenik može provesti privremene mjere zabrane pristupa određenom ili svim resursima 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. O provedenim aktivnostima ili razlozima za nemogućnost postupanja IKT službenik mora odmah obavijestiti predsjednika suda.

(6) 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.

(7) IKT službenik vodi evidenciju koja sadrži relevantne informacije o incidentima, preduzetim mjerama i načinu njihovog rješavanja. Sadržaj evidencije propisuje predsjednik suda na prijedlog IKT službenika.

POGLAVLJE III – ORGANIZACIONE MJERE SIGURNOSTI INFORMACIONOG SISTEMA

Član 16.
(Načela sigurnosti informacionog sistema)

Sigurnost 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 17.
(Zakonitost i poslovne potrebe)

Informacije se unutar 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 Osnovnog suda u Zvorniku.

Nabavka IKT opreme, softverskih rješenja i usluga

Član 18.
(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 Osnovnog suda u Zvorniku koji regulišu provođenje postupaka javnih nabavki.

(2) U procesu podnošenja zahtjeva iz prethodnog stava, podnosilac ima obavezu pribaviti mišljenje IKT službenika. IKT službenik, provjerava zahtjev imajući u vidu postojeću infrastrukturu i softverska rješenja, te podnosiocu zahtjeva u Osnovnom sudu u Zvorniku 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 Zakonom o javnim nabavkama i internim aktima Osnovnog suda u Zvorniku koji regulišu provođenje postupaka nabavki.

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

Član 19.
(Ugovorno uređenje odnosa sa dobavljačem)

(1) Zaključenjem ugovora o isporuci opreme ili pružanju usluga koje mogu biti od uticaja na sigurnost 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 Osnovnog suda u Zvorniku 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 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 Osnovnog suda u Zvorniku i Politikom sigurnosti.

Ljudski resursi

Član 20.
(Dodjela ovlaštenja za pristup resursima, podacima i informacijama u informacionom sistemu)

(1) Predsjednik suda ili osoba koju on ovlasti, pismenim putem dodjeljuje ili oduzima korisnicima ovlaštenja za pristup resursima, podacima i informacijama u informacionom sistemu.

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

(3) IKT službenik 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 IKT službenik, prema sadržaju koji propisuje predsjednik suda.

(5) Najmanje jednom godišnje IKT službenik, dostavlja izvještaj sa imenima korisnika i njihovim pravima pristupa šefovima unutrašnjih organizacionih jedinica Osnovnog suda u Zvorniku, koji potvrđuju ili po potrebi predlažu izmjene prava pristupa shodno stavu (1) ovog člana.

(6) Pravilnikom o kategorizaciji, čuvanju i korištenju podataka, koji donosi predsjednik suda, propisuje se kategorizacija podataka, označavanje podataka, dodjeljivanje prava pristupa podacima, rukovanje podacima i katalog podataka u vlasništvu Osnovnog suda u Zvorniku.

(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 21.
(Izjava o povjerljivosti)

(1) Izjavu o povjerljivosti potpisuju svi zaposleni u Osnovnom sudu u Zvorniku, 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 Osnovnom sudu u Zvorniku je odgovoran za uključivanje klauzule povjerljivosti u ugovor sa ugovaračem ili sa vanjskim saradnikom.

Član 22.
(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) Sudska 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 23.
(Zasnivanje radnog odnosa)

(1) Sudska 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 24.
(Duža odsutnost zaposlenika)

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

(2) IKT službenik, će obavijestiti sudsku upravu o provedenim mjerama po osnovu zahtjeva iz stava (1) ovog člana.

Član 25.
(Gubitak ili otuđenje opreme)

(1) Ukoliko zaposlenik pravosudne institucije izgubi povjerenu mu opremu ili mu ista bude otuđena mora o tome bez odlaganja obavijestiti sudsku 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 sudskoj upravi.

Član 26.
(Prestanak radnog odnosa)

(1) Sudska 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) Predsjednik suda, 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 stava (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. Sudska uprava je zadužena za izvršenje njihovog zaključka.

Član 27.
(Službenik za informacionu sigurnost)

(1) Službenik za informacionu sigurnost u Osnovnom sudu u Zvorniku 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 predsjednika suda 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 Osnovni sud u Zvorniku 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 će biti koordiniran i dobijaće smjernice za rad od službenika za informacionu sigurnost VSTS-a BiH.

POGLAVLJE IV – FIZIČKE I TEHNIČKE MJERE SIGURNOSTI INFORMACIONOG SISTEMA

Član 28.
(Fizička i tehnička zaštita server sobe)

(1) U Osnovnom sudu u Zvorniku se uspostavljaju mjere fizičke i tehničke zaštite u zaštićenom prostoru s ograničenim pristupom – server sobi, u kojoj se nalazi IKT oprema koja omogućava funkcionisanje 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) protivpožarni alarm.

Član 29.
(Servisiranje tehničkih sredstava zaštite server sobe)

(1) O redovnom održavanju i servisiranju tehničkih sredstava zaštite server sobe stara se pružalac usluge s kojim 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 30.
(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 predsjednika suda. Popisi datih ovlaštenja i osoba moraju biti revidirani najmanje jedanput godišnje.

(4) Svaki ulazak u server sobu evidentira se u dnevniku ulazaka, koji vodi IKT službenik. U dnevniku ulazaka evidentira se ovlaštena osoba koja je pristupila server sobi i tačan vremenski period boravka u server sobi.

(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 predsjednik suda, koji će odrediti zaposlenog koji će vanjskog saradnika pratiti sve vrijeme njegovog boravka, odnosno do izlaska iz Osnovnog suda u Zvorniku. 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 predsjednika suda.

Član 31.
(Izvedba elektro i telekomunikacionih instalacija)

Elektro i telekomunikacione instalacije u sudu moraju biti izvedene na način da ih nije moguće nenamjerno prekinuti ili bez većih teškoća uništiti ili zloupotrijebiti.

Član 32.
(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;

(3) Server soba mora imati sistem za automatsku vatrodojavu povezan sa operativnim centrom organizacione jedinice nadležne za sigurnost suda.

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

Član 33.
(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 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 34.
(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 koje donosi šef Odjela za IKT VSTS BiH.

Član 35.
(Upravljanje otpadom)

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

POGLAVLJE V – INFORMATIČKE MJERE SIGURNOSTI INFORMACIONOG SISTEMA

Član 36.
(Operativni postupci i odgovornosti)

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

Član 37.
(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.

Zaštita od zlonamjernih programa

Član 38.
(Zaštita od zlonamjernih programa)

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

Član 39.
(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 40.
(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 41.
(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 vrši se u skladu sa odredbama člana 44. stav (2) i (3) Politike sigurnosti pravosudnog informacionog sistema BiH

Član 42.
(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 IKT službenika.

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

Član 43.
(Sigurnosne nadogradnje operativnog sistema na radnim stanicama i serverima pravosudnog informacionog sistema)

(1) Sve radne stanice i serveri u 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 44.
(Upravljanje dokumentacijom informacionog sistema)

Cjelokupna dokumentacija 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 predsjednika suda;

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 određenim katalogom servisa iz člana 7. 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 sefu suda.

Član 45.
(Sistemska dokumentacija)

(1) IKT službenik obezbjeđuje izradu i ažuriranje sistemske dokumentacije, njenu raspoloživost i zaštitu, za resurse informacionog sistema Suda.

(2) O sistemskoj dokumentaciji svakog pojedinačnog resursa informacionog sistema se brine IKT službenik.

Član 46.
(Pregled i zaštita dnevnika)

(1) Nadzor nad 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 IKT službenik.

(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 VSTS BiH.

(5) Dnevnički zapisi se ne smiju ručno brisati.

Izrada rezervnih kopija sistema i podataka

Član 47.
(Rezervne kopije resursa i podataka)

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

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

(4) IKT službenik je zadužen za izradu backupa sistema i podataka na serverima, 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 suda.

Član 48.
(Čuvanje backupa podataka)

(1) Predsjednik suda 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) Predsjednik suda određuje vanjske lokacije na kojima se čuvaju backupi iz stava (1) ovog člana.

Nosači podataka

Član 49.
(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 VSTS BiH.
(3) Nosače podataka iz stava (1) ovog člana mogu da iznose iz prostorija suda samo za to ovlaštene osobe. Listu ovlaštenih osoba donosi predsjednik suda.
(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 predsjednika suda 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 VSTS BiH.

Član 50.
(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 VSTS BiH.

(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 predsjednik suda na prijedlog 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 suda.

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

Korisnički nalozi i šifre

Član 51.
(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 VSTS BiH donosi posebno tehničko uputstvo kojim se uređuju pravila za kreiranje i upravljanje korisničkim nalozima i šiframa.

Član 52.
(Administrativni i servisni nalozi i šifre resursa 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 imenovani su nadležni administratori VSTS BiH.

(5) Svaka šifra poznata IKT službeniku obavezno se mijenja u slučaju prestanka njegovog radnog odnosa u sudu.

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

Računarske mreže

Član 53.
(Korištenje i sigurnost mrežnih usluga)

(1) Mreža 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 54.
(Upravljanje mrežama pravosudnog informacionog sistema)

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

(2) Sva priključenja računara koji su u vlasništvu Osnovnog suda u Zvorniku, ali nisu dio pravosudnog informacionog sistema, na LAN mrežu pravosudnih institucija, moraju biti odobrena od strane šefa Odjela za IKT VSTS-a.

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

(4) Prije nego što se odobri pristup mrežnim resursima, sva oprema iz stava (3) ovog člana se mora autentifikovati.

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

Član 55.
(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 VSTS BiH.
(4) Način i tehnike korištenja VPN tehnologije se utvrđuju posebnim tehničkim uputstvom koje donosi šef Odjela za IKT VSTS BiH.
(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.

Elektronska pošta i Internet

Član 56.
(Prihvatljiva upotreba elektronske pošte)

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

Član 57.
(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 58.
(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 IKT službenika, koji će dalje o istom da obavijesti Odjel za IKT VSTS-a.

(2) Odjel za IKT će o ovome informisati predsjednika suda 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 predsjednika suda.

(4) U slučaju ponovljene neprihvatljive upotrebe elektronske pošte od strane istog korisnika, odjel za IKT VSTS-a će prema takvom korisniku odmah primijeniti privremenu mjeru zabrane slanja elektronske pošte i o istome obavijestiti predsjednika suda kojoj korisnik pripada.

(5) Zahtjev za ukidanje privremene mjere zabrane slanja elektronske pošte predsjednik suda upućuje Odjelu za IKT VSTS-a pismenim putem. Odjel za IKT VSTS-a će razmotriti zahtjev i obavijestiti predsjednika suda o statusu privremene zabrane slanja elektronske pošte.

Član 59.
(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 60.
(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 61.
(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, predsjednik suda je dužan 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 VSTS-a.

Član 62.
(Prihvatljiva upotreba Interneta)

Pristup Internetu je omogućen u poslovne svrhe.

Član 63.
(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 64.
(Postupak u slučaju uočavanja neprihvatljive upotrebe Interneta)

(1) Odjel za IKT će odmah, kada to uoči, obavijestiti predsjednika suda kojoj pripada korisnik koji je izvršio radnju koja predstavlja neprihvatljivu upotrebu Interneta.

(2) Korisnik koji na neprihvatljiv način upotrebljava Internet biće upozoren od strane predsjednika suda.

(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 predsjednika suda.

(4) Pismeni zahtjev za ukidanje privremene mjere zabrane pristupa Internetu predsjednik suda upućuje Odjelu za IKT, koji će razmotriti zahtjev i obavijestiti predsjednika suda o statusu privremene zabrane pristupa Internetu.

Član 65.
(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 66.
(Fizička i softverska zaštita prenosne opreme)

(1) Korisnici prenosne opreme u vlasništvu suda su dužni preduzeti sve potrebne radnje da bi istu zaštitili od otuđenja i/ili neovlaštenog pristupa.
(2) Odjel za IKT VSTS BiH 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 VSTS BiH donosi tehničko uputstvo kojim se propisuju minimalni standardi softverske zaštite prenosnih uređaja i u njima pohranjenih podataka.

Član 67.
(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 VSTS BiH;
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 68.
(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 69.
(Mogući vanredni događaji)

(1) Predsjednik suda utvrđuje osnovne elemente kriznog upravljanja s ciljem nastavka poslovnih procesa u ograničenom odnosno punom obimu u slučaju vanrednih događaja.

(2) Predsjednik suda osigurava provođenje procjene ugroženosti s prijedlogom mjera za njihovo smanjenje ili otklanjanje.

(3) Predsjednik suda utvrđuje glavne moguće vanredne događaje i procjenjuje vjerovatnoću da do njih dođe.

Član 70.
(Ključni poslovni procesi i zadaci)

(1) Predsjednik suda 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) Predsjednik suda 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 71.
(Podaci za ključne kontakte)

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

Član 72.
(Komunikacija)

(1) Planovi i mjere u slučaju vanrednog događaja u sudu 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 73.
(Zaštitne kopije ključne dokumentarne građe)

(1) Predsjednik suda imenuje osobu odgovornu za zaštitne kopije ključnih dokumenata i zapisa suda.

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

(3) Ako su ključni dokumenti i zapisi u slučaju vanrednog događaja uništeni, predsjednik suda organizuje nastavak poslovanja rekonstrukcijom podataka iz zaštitnih kopija.

Član 74.
(Plan oporavka)

(1) IKT službenik izrađuje plan oporavka (engl. disaster recovery plan) ključnih servisa 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 70. 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 predsjednik suda.

POGLAVLJE VI – PRELAZNE I ZAVRŠNE ODREDBE

Član 75.
(Kršenje odredbi Politike sigurnosti)

(1) U slučaju kršenja odredbi Politike sigurnosti prekršiocu se može izreći mjera zabrane korištenja određenog servisa 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 sudom. U slučaju težih kršenja odredbi Politike sigurnosti može se protiv takvih pravnih ili fizičkih lica pokrenuti odštetni ili drugi postupak pred nadležnim organima.

Član 76.
(Stupanje na snagu)

Politika sigurnosti informacionog sistema Osnovnog suda u Zvorniku stupa na snagu danom donošenja.