BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
FEDERALNA AGENCIJA ZA UPRAVLJANJE ODUZETOM IMOVINOM

P R O C E D U R E I P R A V I L A

KORIŠTENJA, SIGURNOSTI I ZAŠTITE PODATAKA INFORMACIONOG SISTEMA

Sarajevo, septembar/rujan 2018. godine

Na osnovu člana člana 60. Zakona o organizaciji organa uprave u Federaciji Bosne i Hercegovine („Službene novine Federacije BiH", broj: 35/05), a u skladu sa poglavljem III. stav (1) tačka 13. Smjernica za uspostavu i jačanje interne kontrole kod budžetskih korisnika („Službene novine Federacije BiH", broj: 19/05), direktor Federalne agencije za upravljanje oduzetom imovinom, d o n o s i

PROCEDURE I PRAVILA
korištenja, sigurnosti i zaštite podataka Informacionog sistema

I - OSNOVNE ODREDBE

Član 1.
(Predmet)

Procedurama i pravilima korištenja, sigurnosti i zaštite podataka informacionog sistema (u daljem tekstu: Procedure i pravila) propisuje se način i ovlasti za korištenje, sigurnost i zaštitu podataka i fajlova informacionog sistema (u daljem tekstu: IS) Federalne agencije za upravljanje oduzetom imovinom (u daljem tekstu: Agencija).

Član 2.
(Značenje pojmova)

Izrazi korišteni u ovim procedurama imaju slijedeća značenja:

1) **Informacioni sistem** - je integrisani skup komponenti za sakupljanje, snimanje, čuvanje, obradu i prenošenje informacija;
2) **Administrator mreže** - je osoba zadužena za održavanje i upravljanje IT sistemom, odnosno računarskim sistemom i mrežom;
3) **Korisnička grupa** - je grupa korisnika koja je klasifikovana prema pravima pristupa i ovlaštenjima za rad na mreži;
4) **Hardver** - je materijalna osnova - računar, ulazno-izlazni uređaji, dio uređaja za komuniciranje i prijenos podataka, i ostala računarska oprema (pisač/štampač, radne stanice, telekomunikacijska oprema i dr.) namijenjeni obradi podataka, odnosno informacija;
5) **Softver** - predstavlja nematerijalne elemente, a to su programi, biblioteke i kolekcije podataka koji govore računaru kako da radi;
6) **Aplikacija** - je softver dizajniran da izvršava grupu koordiniranih funkcija, taskova ili aktivnosti u za dobrobit korisnika (e.g. Microsoft Word, Paint, Mail);
7) **Server** - je računar ili računarski sistem koji pruža usluge drugim računarima ili računarskim sistemima – klijentima;
8) **Klijent** - je najčešće korisnički računar ili program koji komunicira sa udaljenim računarom-serverom;
9) **Folder** - je mjesto na disku namjenjeno za smještanje podataka;
10) **Dijeljeni folder** - je folder kreiran za razmjenu podataka na mreži;
11) **Šering** - je opcija kojom se folder čini dostupan drugom;
12) **HDD–Hard Disk Drive** - je uređaj za pohranjivanje i čitanje podataka. Njegove osnovne karakteristike su kapacitet i brzina pisanja/čitanja;
13) **Particija diska** - je dio HDD-a ukoliko je HDD podijeljen u dijelove ili neki eksterni prostor za pohranjivanje pri čemu operativni sistem može upravljati particijama odvojeno te na njih pohranjivati podatke;
14) **Mbps** - je znak za megabit u sekundi (milijun bita u sekundi), mjerna jedinica za brzinu prijenosa podataka u informatici i komunikacijama;

15) **PDF** - Portable Document Format, je univerzalni format elektronskih dokumenata koji se mogu prenositi sa računara na računar pri čemu se zadržava originalni izgled stranice, sa svim fontovima, slikama ili tabelama;
16) **Internet** - je javno dostupna globalna mreža koja zajedno povezuje računare i računarske mreže korištenjem istoimenog protokola (internet protokol = IP);
17) **IP**- Internet Protocol, je mrežni protokol za prijenos podataka kojeg koriste izvorišna i odredišna računala za uspostavu podatkovne komunikacije preko računalne mreže;
18) **RAM** - Random Access Memory (memorija nasumičnog pristupa), je jedan od oblika pohranjivanja računarskih podataka čijem sadržaju se može pristupiti po bilo kom redoslijedu;
19) **CPU** - Central Processing Unit je elektronska komponenta napravljena od minijaturnih tranzistora na jednom čipu (poluprovodničkom integralnom sklopu) koja radi prema instrukcijama kompjuterskih programa tako što izvodi osnovne artimetičke, logičke kontrolne i I/O (Input/Output) operacije;
20) **XML** - EXtensible Markup Language – je strukturirani jezik za opisivanje sadržaja, odnosno podataka;
21) **HTTPS** - Hyper Text Transfer Protocol Secure, omogućava kriptovanu komunikaciju i sigurnu identifikaciju web poslužitelja mreže;
22) **SSL** - Secure Sockets Layer, omogućava sigurnu komunikaciju preko Interneta za razne aplikacije;
23) **Web servis** - je metoda za komunikaciju između dva elektonička uređaja putem Interneta;
24) **Replikacija** - je kreiranje i održavanje višestrukih kopija iste baze podataka;
25) **Verifikacija** - Provjera i potvrda vjerodostojnosti i istovjetnosti podataka unesenih u matični registar(u elektronskoj bazi podataka) i matičnoj knjizi u fizičkom obliku;
26) **Zaštitino memorisanje** - (backup, pohranjivanje podataka) je postupak izrade i pohranjivanja (snimanja) sigurnosne kopije podataka na prenosive magnetske ili optičke medije, za slučaj gubitka, oštećenja ili uništenja podataka;
27) **Switch** - mrežni uređaj koji povezuje uređaje u jednoj mreži koristeći njihovu fizičku (MAC) adresu te omogućava razmjenu podataka između uređaja koji su spojeni na isti switch;
28) **Ruter** - mrežni uređaj koji povezuje različite mreže koristeći IP adresu te omogućuje razmjenu podataka između različitih mreža;
29) **Intranet** - privatna mreža kojoj mogu pristupiti samo korisnici te mreže (e.g. Mreža kompanije kojoj mogu pristupiti samo uposlenici kompanije dok su u kompaniji). Malene mreže poput onih u kompanijama se nazivaju Lokalnim (LAN – Local Area Network) dok se mreže koje obuhvataju velike površine nazivaju Širokim mrežama (WAN – Wide Area Network);
30) **„particija diska“**: podaci se mogu snimati na disk C: ili disk D: Oba ova diska spadaju u kategoriju „tvrdi disk“ kompjutera.

II – INFORMACIONI SISTEM AGENCIJE

Član 3.
(Cilj)

IS Agencije je ustrojen tako da pruža učinkovitu pomoć u obavljanju poslova operacija i zadovoljava različite potrebe korisnika.

Osnovni ciljevi sigurnosti informacionog sistema su:

- ❖ Povjerljivost podataka – glavni cilj IS-a. Odnosi se na sprječavanje povjerljivih informacija da dođu u ruke neautorizovanih korisnika.
- ❖ Integritet podataka – sprječavanje neautorizovanih korisnika da izmjene podatke bilo da se radi o neautorizovanim korisnicima (hakerima) ili autorizovanim korisnicima koji pokušavaju modifikovati podatke koje ne bi trebali
- ❖ Dostupnost – resursi i informacije su lako dostupne svim autorizovanim korisnicima sistema.

Kako bi mrežni sistem bio stabilan i resursi uvijek bili na raspolaganju, koriste se standardizovane radne stanice. Standardizacija uključuje hardver, operativni sistem i aplikacije, kao i rukovodeće aspekte radnih stanica.

Član 4.
(Infrastruktura Informacionog sistema)

Infrastruktura IS-a Agencije obuhvata sljedeće:

- ❖ prijenosno računar (laptop), mrežne radne stanice, pisače, poslužitelje (servere), baze podataka;
- ❖ aktivnu mrežnu opremu kao što su swichevi, routeri, modemi i drugo;
- ❖ komunikacijski linkovi za pristup serveru i mrežnim uređajima;
- ❖ upravljačke servise koji uključuju elektronsku poštu, korištenje softvera, intraneta i pomoći korisnicima.

Kompletan sistem uključuje: WAN (distribuiranu mrežu) i LAN (lokalnu mrežu), koja omogućava distribuiranu obradu podataka i dijeljenje resursa, te pristup internetu.

III – SIGURNOST INFORMACIJA NA RADNIM STANICAMA

Član 5.

Podaci i informacije koje se smatraju bitnim i povjerljivim za obavljanje upravnih, stručnih i drugih poslova koji su zakonom i drugim propisima stavljeni u nadležnost Agenciji uživaju zaštitu, na način i pod uslovima propisanim ovim Procedurama.

Član 6.
(Radne stanice i pisači)

Radne stanice (računari) namijenjene su isključivo poslovnoj upotrebi. Zaposleni koriste radne stanice na kojima ne mogu mijenjati konfiguraciju i koje su podešene na identičan način kod svih korisnika u skladu sa potrebama radnih procesa koji diktiraju postavke radnih stanica. Korisnici ne mogu ukloniti ili mijenjati određene sistemske postavke radnih stanica, niti dodavati nove bez odobrenja direktora Agencije.

Zabranjeno je spajanje računara ili bilo kakve opreme na informacioni sistem, osim u izuzetnim slučajevima i uz odobrenje direktora Agencije.

Nabavka radnih stanica odvija se samo prema specifikaciji koju priprema Sektor za pravne i opće poslove i prema procedurama javnih nabavki.

Prijenosni računari su dio IS-a i mogu biti korišteni kao zamjena za radne stanice ili privremeno (npr. za poslovno putovanje). Za dodatno korištenje prijenosnih računara, pored postojeće radne stanice, za jednog korisnika potrebno je imati pismeno odobrenje direktora Agencije. Kao takvi oni sadrže povjerljive informacije o IS-u i iz sigurnosnih razloga o njima treba voditi posebnu brigu.

Član 7.
(Softver na radnim stanicama)

Na svim radnim stanicama instaliran je softver u skladu sa potrebama za određenim poslom. Specifikacije za standardni operativni sistem radnih stanica godišnje se podešavaju da bi pratile razvoj u industriji informacionih tehnologija. Operativni sistem koji zaposleni trenutno koriste je Microsoft Windows 10.

Zbog mogućih kršenja autorskih prava, te rizika za IS, zabranjeno je koristiti piratski (nezakonit) softver, odnosno softver koji nema zakonitu dokumentaciju i licencu za korištenje.

Korisnik niti može, niti smije instalirati softver ukoliko mu to nije instalirano ili dozvoljeno od direktora Agencije. Stoga korisničke privilegije ne dozvoljavaju korisniku instaliranje softvera.

Ako se na radnoj stanici pronađe instaliran neodobren, nestandardni softver, koji je instalirao korisnik, izvršit će se reinstalacija standardne konfiguracijske radne stanice, a korisnik radne stanice biće pozvan na odgovornost.

Dozvoljeni softver za radne stanice je:

1. Microsoft Windows 10 ili Windows 7
2. Microsoft Office 365,
3. Antivirusni program,
4. Microsoft Internet Explorer,
5. Adobe Acrobat Reader,
6. Softverski paketi za uredsko i finansijsko poslovanje.

Ako je zbog obaveza korisnika potreban drugi softver, zahtjev za nabavkom i instaliranjem takvog softvera mora odobriti direktor Agencije.

Ukoliko je bilo koji drugi softver, osim spomenutog, već instaliran, on mora biti uklonjen. Stručni savjetnik za informatiku zadužen je za uklanjanje takvog softvera. Zbog potrošnje mrežnih resursa i sigurnosnih razloga, Sektor za pravne i opće poslove izdat će listu zabranjenih softvera koji ne smiju biti instalirani na radne stanice ili prijenosne računare (eMule, Ares, BitTorrent, LimeWire, Morpheus, BearShare's, Google Toolbar, Yahoo Toolbar, Web Shots Screen Saver, razni „add-ons", a naročito programi za skidanje i gledanje multimedijalnih sadržaja s interneta koji ugrožavaju i usporavaju rad mreže).

Sektor za pravne i opće poslove vodi računa o kreiranju radne dokumentacije i redovnom zapisivanju svih promjena koje se tiču softvera. Tu se, prije svega, misli na zahtjeve za pojedinim izmjenama i izvršene promjene na postojećim softverima, nabavku novog i zamjenu starog softvera.

Član 8.
(Korisnički računi i šifre)

Da bi korisnik pristupio sistemu preko radne stanice, potrebno je da ima važeći korisnički račun koji uključuje korisničko ime i šifru. Svakom korisniku kreira se korisnički račun s dodijeljenom početnom šifrom. Kod prvog prijavljivanja na sistem korisnik je dužan promijeniti inicijalno dodijeljenu mu šifru. Šifra mora biti promijenjena najmanje jednom u tri mjeseca, mora biti tajna, i u slučaju pisane kopije treba je čuvati „pod ključem". Korisnička šifra ne smije se dijeliti ni s kim.

Korisnički računi su osnov pristupne politike informacijama. Korisnički računi koriste se za reviziju pristupa resursima i za verifikovanje identiteta zaposlenih u automatskim poslovnim procesima, i radi toga se trebaju kreirati samo lični računi. Korisnički račun je jedinstven i jedna osoba može imati samo jedan korisnički račun koji će biti prepoznatljiv tako što će se sastojati od imena.prezimena.

Osmišljavanje korisničke šifre odgovornost je korisnika, a pri tome se moraju uvažavati sljedeća načela:

a. Šifra treba sadržavati najmanje osam karaktera i to kombinacija velikih i malih slova, brojeva i posebnih znakova;
b. Šifra ne smije sadržavati korisničko ime (adresu elektronske pošte) ili bilo koji oblik ličnog imena;
c. Šifra ne bi trebala biti „obična" riječ, odnosno pojam iz svakodnevnog govora ili kompletna riječ iz bilo kojeg jezika;
d. Šifra mora biti promijenjena nakon 90 dana.

Zabranjeno je korištenje BIOS-a, odnosno „power-on" šifre.

Šifrom zaštićen zaštitnik zaslona (Screen Saver) – zaključavanje ukoliko korisnik ne koristi računar – aktivira se nakon 30 minuta. Ponovni postupak korisnik će imati unošenjem šifre.

Član 9.
(Administratorska šifra sistema)

Administratorske šifre sistema ima osoba odgovorna za održavanje računarske opreme. Administratorska šifra smatra se službenom tajnom i uz zapisnik se čuva u zapečaćenoj koverti u sefu i mijenja se svakih šest mjeseci, uz poštivanje procedura pečaćenja i pohranjivanja u sigurnosni sef. Ukoliko se koverta sa šifrom nađe pocijepana ili oštećena, o tome se obavještava direktor Agencije.

Član 10.
(Zaboravljanje šifri)

Ako zaposleni zaboravi svoju šifru, osoba odgovorna za održavanje računarske opreme nije u mogućnosti istu šifru ponovo vratiti. U takvim slučajevima potrebno se pismeno obratiti administratoru i zahtijevati dodjelu nove šifre.

Administrator neće resetovati šifru za zaposlenog na osnovu zahtjeva neke druge osobe, koja nije vlasnik računa. Svako mijenjanje šifre administrator je dužan zapisati u svoj administrativni dnevnik, u koji evidentira resetovanje i zamjenu šifre.

Član 11.
(Blokada računa)

Ako se za bilo koji račun unosi pogrešna šifra uzastopno tri puta, račun će se automatski podesiti na „blokiran" zbog sigurnosnih razloga jer je to mogući nedopušten ulazak. Kada se zaposleni želi prijaviti (log in), nakon što je sistem blokirao njegov račun, pristup mreži odbijen je i korisnik će o tome biti obaviješten.

Procedura za resetovanje šifre ista je kao u slučaju zaboravljene šifre. Administrator će istražiti i označiti taj račun kao onesposobljen u slučaju nedopuštenih radnji. Neprihvatljiva je praksa davanja šifre povjerljivim osobama (saradniku, pomoćniku itd.) jer u slučaju bilo kakve zloupotrebe svaki korisnik snosi odgovornost za zloupotrebu nastalu korištenjem vlastitog računa.

Član 12.
(Backup sistema – sigurnosna kopija)

1. Administrator mreže dužan je voditi računa o pravljenju rezervnih kopija na serveru, kao i njihovoj zaštiti.

2. Administrator mreže je dužan trenutno, jednom dnevno, sedmično, mjesečno ili godišnje praviti sigurnosne kopije (backup) svih važnijih dokumenata i baza podataka na prenosivom disku (floppy; CD; USB memory stick) i iste pohranjivati na sigurnom mjestu.

3. Prenosivi diskovi sa povjerljivim podacima ne smiju se iznositi izvan Agencije i ne smiju se nositi klijentima.

IV – ZAŠTITA OD VIRUSA

Član 13.

Za zaštitu od virusa zadužen je Stručni savjetnik za informatiku koji je obavezan:

- da na svim kompjuterima izvrši instaliranje antivirusnog softvera,
- da izvrši blagovremenu nadogradnju.

Član 14.

Svaki Korisnik je dužan, da:

- koristi antivirusni softver,
- da sve zaražene fajlove očisti, i da o svim potencijalnim problemima obavijesti administratora mreže.

Član 15.

Ukoliko je računar spojen na internet obavezno se na taj računar treba aktivirati firewall koji će sistem štititi od neovlaštenih upada.

Član 16.

Ako se radi o mreži računara koji se preko servera ili nekog drugog računara spajaju na internet, firewall aktivirati samo na server ili računar direktno spojen na Internet.

V – PRISTUP INTERNETU

Član 17.
(Korištenje interneta)

Pristup internetu je odobren i ograničen za poslovne potrebe, i biće blokiran u slučaju otkrivanja zloupotrebe.

Agencija održava internetsku vezu za poslovne svrhe. Kao što je slučaj i s elektronskom poštom, dozvoljeno je umjereno korištenje za lične potrebe. Neprihvatljivo korištenje kapaciteta interneta biće prijavljeno direktoru Agencije kako bi se problem otklonio.

Primjeri neprihvatljivog korištenja uključuju:

- skidanje (download) ili slanje (upload) datoteka i materijala zaštićenih autorskim pravima, kao što su: softver, audio i video;
- pristupanje, skidanje ili prijenos materijala nepristojnog sadržaja, kao naprimjer pornografskog materijala;
- korištenje veza koje nije povezano s poslom, kao što je audio i videostreaming.

Pristup internetu je namjenjen za korištenje zakonom dopuštenih aktivnosti. Prijenos, spremanje, distribucija informacija, podataka ili materijala kojim se krše bilo koji zakoni ili odredbe je strogo zabranjeno. To uključuje, ali se ne ograničava na: materijal zaštićen copyrightom, trademark, poslovna tajna ili ostalo intelektualno vlasništvo ili pravo korišteno bez autorizacije i materijal koji je prost, uvredljiv, predstavlja nezakonitu prijetnju, ili krši zakone kontrole izvoza.

Primjeri neprihvatljivog sadržaja ili linkova:

- Piratski programi;
- Piratski servisi za gledanje filmova;
- Hackerski programi ili arhive;
- Warez stranice;
- Skidanje pjesama i igrica.

Član 18.

Pristup internetu s prijenosnog računara putem drugih internetskih providera je moguć. Korisnik mora imati otvoren pretplatnički račun kod nekog internetskog providera kako bi ova usluga bila moguća. Prije instaliranja bilo kakvih korisničkih računa na prijenosnim računarima, korisnik mora podnijeti pismeni zahtjev Sektoru za pravne i opće poslove s napisanim pristupnim podacima dobijenim od internetskog providera kako bi mu osoba zadužena za IT-a navedenu pristupnu konekciju postavilo na prijenosni računar.

Zabranjeno je lažno predstavljanje korisnika, prikrivanje, zatajenje ili izostavljanje ličnog ili drugog korisničkog identiteta u okviru informacionog sistema Agencije.

Korisničko ime, adresa elektronske pošte, organizaciona afilacija i povezane kontakt informacije uvijek moraju prikazivati pošiljatelja poruke. Korištenje anonimnosti ili nekog prikrivanja identiteta strogo je zabranjeno, osim u slučajevima autorizacije od pomoćnika direktora Sektora za pravne i opće poslove.

Član 19.
(Dijeljenje direktorija)

Korisnici ne mogu dijeliti direktorije na internetu. Ako postoji potreba da se informacije dijele sa saradnicima, biće zatražena pomoć osobe zadužene za IT-a. Takođe se ne smiju prihvatati nepozvane datoteke zbog mogućeg rizika od virusa. Skinute datoteke s interneta mogu sadržavati skrivene viruse koji mogu učiniti resurse računara dostupnim putem internetske veze.

Uopće, povjerljive informacije ne smiju biti puštene izvan Agencije. Ukoliko je potrebno prebaciti ili distribuirati takve informacije, obaveza je zaštiti ih odobrenom enkripcijskom metodom.

Korisnik ne smije slati nikakve osjetljive parametre Agenciji koji bi mogli ugroziti sigurnost sistema, kao što su broj bankovne kartice, bilo koje šifre ili broja korisničkog računa putem interneta.

VI – ELEKTRONSKA POŠTA (E-MAIL)

Član 20.
(Elektronska pošta)

Elektronska pošta se koristi kao vid komunikacije između zaposlenih, kao i sa drugima izvan Agencije. Ovaj vid komunikacije smatra se službenim i obavezujućim za sve zaposlene.

Svi zaposleni imat će adrese elektronske pošte u jedinstvenoj formi: ime.prezime@fazuoi.gov.ba.

Korisnici su dužni provjeravati elektronsku poštu najmanje jednom tokom svakog radnog dana. Kada iz operativnih razloga korisnik nije u mogućnosti koristiti svoj računar, dužan je pristupiti svojoj elektronskoj pošti s drugog računara.

Poštanski pretinci (mailbox) se čuvaju na poslužiocu elektronske pošte (mail server) i dozvoljen im je pristup putem Microsoft Outlooka ili putem web-stranice. Nove poruke će prema konfiguraciji dolaziti u mapi (folderu) ulazne pošte (inbox). Korisnici su dužni čuvati svoju elektronsku poštu.

Poslužioc elektronske pošte (server) je ograničen kapacitetom prostora za smještanje podataka te je količina elektronske pošte koja može biti čuvana na poslužiocu limitirana. Zato korisnici moraju voditi računa o veličini svojih poštanskih pretinaca. U slučaju da se poštanski pretinac napuni, automatski se zatvara i elektronska pošta ne može stizati u njega dok ga korisnik ne isprazni. Preporučuje se korištenje Outlook-a, gdje se aktivira automatsko brisanje pošte sa servera: korisnik svu poštu zadržava na vlastitom računaru, dok se pošta briše sa servera.

Član 21.
(Zaštita)

Pokazalo se da je elektronska pošta glavni prenosilac zlonamjernih napada na kompjuterske mreže. Raspon ovih napada kreće se od „poplava“ elektronske pošte do virusa koji briše informacije na mašini. Zabranjeno je slati ili prosljeđivati bilo kakvu vrstu upozorenja o mogućoj prijetnji elektronske pošte.

Za elektronsku poštu obavezno je provođenje antivirusnog sigurnosnog sistema.

VII – KORIŠTENJE WEB-STRANICE AGENCIJE

Član 22.
(Komunikacija putem web-stranice)

Web-stranica se koristi kao vid komunikacije Agencije i javnosti, stoga je veoma bitno da su informacije koje se objavljuju na web-stranici vjerodostojne. Na osnovu važnosti informacija objavljenih na web-stranici, samo ovlaštena osoba Agencije, ima pravo odobriti koje informacije mogu ići na web-stranicu, a samo administrator web-stranice može postavljati/skidati informacije sa web-stranice.

Ovaj vid komunikacije smatra se službenim i obavezujućim za sve zaposlene.

Član 23.
(Procedure objavljivanja informacije)

Procedure objavljivanja informacije na web-stranicu:

a) informacija za objavljivanje na web-stranicu dostavlja se osobi zaduženoj za pregled informacije;
b) nakon što osoba zadužena za pregled informacije odobri navedenu informaciju, prosljeđuje je na elektronsku poštu administratoru web-stranice;
c) po primanju informacije, administrator web-stranice provodi postavljanje informacije na web-stranicu; isto načelo važi, po upućenom zahtjevu, za skidanje (brisanje) informacija s web-stranice.

Član 24.

Dokument koji treba staviti na web-stranicu potrebno je dostaviti administratoru web-stranice najmanje jedan dan (24 sata) prije vremena objave navedene informacije na web-stranici. Izuzetak od navedenog su slučajevi kada je potrebno pojedine informacije hitno postaviti na web-stranicu.

Tada osoba zadužena za pregled informacije pismeno ili elektronskom poštom prosljeđuje administratoru zahtjev za hitno postavljanje informacije na web-stranicu.

VIII – KORISNICI I UPOTREBA IS-a AGENCIJE

Član 25.
(Korisnici informacionog sistema)

Korisnici IS-a Agencije su uposleni u Agenciji.

Član 26.
(Sredstva informacionog sistema)

Sredstva IS-a Agencije vlasništvo su Agencije i mogu se koristiti samo u poslovne svrhe. Obaveza je svih korisnika koristiti sredstva IS-a Agencije na profesionalan, zakonit i etičan način.

Obzirom na ograničenja kapaciteta sredstava IS-a Agencije, posebno mrežnog i memorijskog, svi korisnici imaju obavezu njihovog čuvanja.

Korisnici ne smiju namjerno trošiti i nekorektno koristiti sredstva IS-a Agencije ili ih monopolizirati.

Član 27.

U skladu sa etičkim standardima nije dozvoljeno:

a. prikazivati, čuvati ili distribuirati pornografske tekstove, slike ili bilo koje grafičke ili multimedijalne sadržaje tog tipa;
b. prikazivati, čuvati ili distribuirati materijale koji promovišu seksualno iskorištavanje ili diskriminaciju, rasizam i nasilje;
c. prikazivati, čuvati ili distribuirati poruke koje vrijeđaju rasnu, starosnu, spolnu, religijsku, nacionalnu ili seksualnu pripadnost;
d. prikazivati, čuvati ili distribuirati informacije o oružju i nasilju;
e. prikazivati, čuvati ili distribuirati destruktivne računarske materijale (viruse, spywere, self-replicating programe i drugo);
f. prikazivati, čuvati ili distribuirati masovnu elektronsku poštu (mass mailove), neželjenu poštu (spam mailove) ili lančana pisma;
g. distribuirati lične oglase i promocije poput kupovine roba i primanja usluga na vezi (online);
h. distribuirati komercijalne reklame;
i. prikazivati, čuvati ili distribuirati bilo kakve materijale koji promovišu političke stranke, skupljanje sredstava za iste, kao i druge političke aktivnosti;
j. prikazivati, čuvati ili distribuirati bilo kakav neautorizovani materijal.

Član 28.

Sredstva IS-a Agencije ne smiju biti korištena za prikazivanje, čuvanje ili slanje (elektronskom poštom ili bilo kojom drugom formom elektronske komunikacije kao što su bulletin bord, chat room, UseNet skupine) materijala koji su obmanjujući, uznemirujući, neprilični, seksualno eksplicitni, profani, sramotni, zastrašujući, klevetnički ili drugačije neprikladni i nezakoniti.

U izuzetnim slučajevima u kojima je potrebna zakonska upotreba navedenog zabranjenog materijala, potrebno je prvo zatražiti pisanu autorizaciju pomoćnika direktora Sektora za pravne i opće poslove.

Nezakonito kopiranje je zabranjeno, odnosno korisnici ne smiju kopirati materijale zaštićene autorskim pravima ili bilo kakve povjerljive materijale ili učiniti te materijale dostupnim drugima za kopiranje.

Član 29.

Korisnici su odgovorni za poštivanje zakona o autorskim pravima i zakonitosti licenci koje se odnose na softvere, datoteke, grafičke materijale, dokumente, poruke i druge materijale koji mogu biti preuzeti (download) ili prekopirani.

Sa ciljem očuvanja slike javnosti o Agenciji korisnici ne smiju objavljivati informacije koje se odnose na Agenciju putem interneta, bilo putem javnih grupa za raspravu ili chat grupa, ukoliko taj materijal nije odobrila ovlaštena osoba Agencije.

Korisnici koji objave bilo kakav materijal na internetu, a koji Agencija smatra neprikladnim i potencijalno štetnim, biće predmet disciplinskog postupka.

Agencija je zakonski vlasnik svih informacija čuvanih ili distribuiranih putem računarskih resursa Agencije sa izuzetkom materijala u javnom vlasništvu treće strane.

Član 30.

Korisnici sredstava IS-a Agencije ne smiju biti uključeni u sljedeće aktivnosti:

a) kreiranje lažnih podataka ili podataka koji navode na pogrešno mišljenje;
b) omogućavanje pristupa sredstvima IS-a Agencije licima koja za to nemaju autorizaciju;
c) korištenje sredstava IS-a Agencije suprotno pravima i obavezama zaposlenih u Agenciji;
d) brisanje, oštećenje, trošenje, mijenjanje, skrivanje ili zabranjivanje podataka IS-a Agencije;
e) pokušavanje, pomaganje ili poticanje bilo kakvih zabranjenih aktivnosti.

Član 31.

Neodgovorno korištenje sredstava IS-a Agencije nije dozvoljeno, jer se ona tako troše ili monopoliziraju na štetu drugih. Ovo uključuje ali nije ograničeno samo:

a) na skidanje igara ili softvera za zabavu;
b) na igranje online igara;
c) na zanimanje online chat skupinama;
d) na slanje ili skidanje velikih datoteka;
e) na slušanje radia preko interneta;
f) na korištenje VoIP programa;
g) na streaming audio i video fileova, osim u poslovnu svrhu gdje je potrebno dobiti pismenu suglasnost direktora Agencije;
h) na korištenje automatskih informaciono-distribucionih servisa;
i) na korištenje peer-to-peer klijenata i messengera, na pristup podacima Agencije bez autorizacije.

Član 32.

Agencija zadržava pravo nadziranja i bilježenja bilo kakvih aspekata sredstava IS-a Agencije, uključujući ali ne i ograničavajući se:

a) na sadržaje pojedinačnih osobnih računara;
b) na posjećene chat skupine, news skupine i druge internetske stranice;
c) na skinute datoteke;
d) na svu elektronski poslanu i primljenu poštu.

Agencija zadržava pravo upotrebljavanja bilo kojeg softvera kojim može identificirati i blokirati pristup internetskim stranicama neprikladnim i opasnim po sistem.

IX - ZAVRŠNE ODREDBE

Član 33.
(Nadzor i evidentiranje aktivnosti)

Nadzor i evidentiranje aktivnosti uposlenih na IS-u, te pretraživanje srodnih informacija dozvoljeni su kada postoji zakonska potreba institucije, uključujući ali ne i ograničavajući se:

a) na sumnju o kršenju politike i zabranjene aktivnosti;
b) na održavanje IS-a;
c) na nedostupnost uposlenog.

Član 34.
(Odgovornost za nadzor, evidentiranje i pretraživanje)

Nadzor, evidentiranje i pretraživanje u slučajevima navodnog kršenja politike ili nezakonitih aktivnosti odobrava direktor Agencije.

Nadzor, evidentiranje i pretraživanje može odobriti i osoba ovlaštena od strane direktora Agencije, te zatražiti i angažman vanjskog stručnjaka IT-a na tim poslovima.

Tehnička realizacija ovih aktivnosti bit će dodijeljena pomoćniku direktora Sektora za pravne i opće poslove.

Pretraživanje korisničkih informacija u vlasništvu Agencije, osim autoru, može biti omogućeno u slučajevima kada korisnik napusti Agenciju, duže odsustvuje ili bude nekako drugačije onemogućen duže vrijeme pristupati elektronskim podacima. Autorizaciju za to može dati samo direktor Agencije, a na osnovu pisanog obrazloženja pretpostavljenog od korisnika.

Član 35.
(Odgovornost za primjenu i nadzor)

Za pravilnu primjenu Procedura i pravila, zaduženi su uposleni u skladu sa Pravilnikom o unutrašnjoj organizaciji Agencije, a za nadzor nad primjenom Procedura i pravila odgovoran je direktor Agencije.

Član 36.
(Stupanje na snagu)

Procedure i pravila stupaju na snagu danom donošenja, a objavit će se na web portalu Agencije.

Broj: 01-34-408/18
Sarajevo, 07.09.2018. godine

D I R E K T O R

Kenan Kapo