Bosna i Hercegovina
Federacija Bosne i Hercegovine
Kanton _____
Općina _____

NACRT

P R A V I L N I K
O INFORMATIČKOJ I FUNKCIONALNOJ ZAŠTITI RAČUNOVODSTVENOG SISTEMA GLAVNE KNJIGE TREZORA I POMOĆNIH KNJIGA MODULA

April, 2011. godine

Na osnovu člana 18. stav 2. Zakona o izmjenama i dopunama zakona o trezoru u Federaciji BiH (Sl. Novine F BiH, br.: 79/07), člana 10. Pravilnika o uspostavljanja i vođenju glavne knjige trezora općine i člana _____. statuta općine _____ (sl. _____, br.:_____), Načelnik donosi

P R A V I L N I K
O INFORMATIČKOJ I FUNKCIONALNOJ ZAŠTITI RAČUNOVODSTVENOG SISTEMA GLAVNE KNJIGE TREZORA I POMOĆNIH KNJIGA MODULA

(Opće odredbe)

Član 1.

Ovim Pravilnikom se propisuju tehničke i organizacione mjere koje se odnose na sigurnost podataka i mjere za pohranjivanje i povrat pohranjenih podataka u slučaju gubitka, oštećenja ili uništenja podataka koje Općina mora primijeniti u okviru zaštite računovodstvenog sistema glavne knjige Trezora i pomoćnih knjiga (u daljem tekstu: Jedinstvenog sistema), prijem i obrada, zaštita i distribucija obrađenih podataka, u uslovima računarske obrade podataka.

Član 2.

(1) Obrada i dinamika obrade podataka se obavljaju prema pozitivnim zakonskim propisima i standardima iz oblasti računovodstva.
(2) Promjena dinamike obrade vrši se uz saglasnost rukovodioca organa ili od njega ovlaštenog lica.

Član 3.

Za sve podatke na memorijskim medijima sprovodi se zaštita u skladu sa predviđenim mjerama navedenim u ovom Pravilniku.

Član 4.

(1) Nakon završene obrade, liste i izvještaji predviđeni aplikacijama se štampaju propisanom dinamikom i u propisanom obimu. Štampani materijal se razvrstava po vrstama i korisnicima nakon čega se distribuira korisnicima.
(2) Po prethodno pribavljenoj saglasnosti rukovodioca organa ili institucije ili od njega ovlaštenog lica u skladu sa pozitivnim zakonskim propisima iz oblasti računovodstva, utvrđuju se način i rokovi distribucije štampanog materijala.
(3) Štampani izvještaji ili datoteke iz arhive dostavljaju se korisnicima, u skladu sa odgovarajućim nalogom, uz potvrdu prijema.

(Uloga i dužnosti Općine/Sistem Administratora)

Član 5.

Općina/ Sistem administrator ili drugo ovlašteno lice je odgovorano za čuvanje i sigurnost podataka računovodstvenog sistema glavne knjige trezora i pomoćnih knjiga modula, što podrazumijeva:

(1) Zaštitu od neovlaštenog pristupa ili manipulacije bazom podataka Jednistvenog sistema od strane internih i eksternih korisnika;
(2) Upravljanje korisničkim računima, pravima pristupa i bilježenjem događaja u bazi podataka Jedinstvenog sistema;
(3) Politiku korisničkih lozinki i korisničkih imena za bazu podataka Jedinstvenog sistema;
(4) Uspostavu politike i postupaka za mrežnu sigurnost kako bi se mogućnost sigurnosnih incidenata u bazi podataka Jedinstvenog sistema svela na minimum;
(5) Zaštitu baze podataka Jedinstvenog sistema od virusa i ostalih oblika malicioznih kodova;
(6) Osiguranje prenosa podataka iz Jedinstvenog sistema internim i eksternim korisnicima;
(7) Pohranu podataka i upravljanje sigurnosnim kopijama baze podataka Jedinstvenog sistema;
(8) Kontrolu nad prenosom podataka Jedinstvenog sistema izvan prostorija Server sobe na prenosivim elektronskim medijima kao što su hard diskovi, USBmemorije, DVD-ovi i CD-ovi, osim u slučajevima kada to odobri načelnik općine;
(9) Politiku prenosnih računara u pogledu pristupa bazi podataka Jedinstvenog sistema i pohrane podataka Jedinstvenog sistema;
(10) Osiguranje kontinuiteta aktivnosti u slučaju požara, poplave, zemljotresa ili druge nepogode koja se smatra rezultatom više sile (u daljnjem tekstu: nepredviđene okolnosti) i koja dovodi do neuobičajenog prekida u radu Informacionog sistema;
(11) Zaštitu podataka u slučaju nepredviđenih okolnosti;
(12) Povrat pohranjenih podataka u slučaju gubitka, oštećenja ili uništenja računarske opreme Jedinstvenog sistema;
(13) Testiranje baze podataka Jedinstvenog sistema radi otkrivanja sigurnosnih problema na redovnoj osnovi i nakon instaliranja novih verzija baze podataka Jedinstvenog sistema;
(14) Instaliranje softverske nadogradnje radi uklanjanja sigurnosnih problema koji se ustanove na Jedinstvenom sistemu ili na povezanom softveru;
(15) Praćenje sigurnosnih incidenata u bazi podataka Jedinstvenog sistema radi poduzimanja korektivnih mjera;
(16) Upravljanje sigurnosnim incidentima, edukacija i obuka svih ovlaštenih osoba radi sticanja potrebnog znanja o čuvanju i sigurnosti podataka;
(17) Fizički pristup i zaštita baze podataka Jedinstvenog sistema i računarske opreme;i
(18) Održavanje računarske opreme Jedinstvenog sistema.

(Ovlaštene osobe i pristup bazi podataka Jedinstvenog sistema)

Član 6. (*opcioni dio člana)*

Sistem Administrator ili drugo ovlašteno lice je dužno osigurati da pristup Jedinstvenom sistemu imaju samo ovlaštene osobe. Ovlaštena osoba ne smije prenositi svoja ovlaštenja na drugu osobu, niti svoje ovlasti učiniti dostupnim drugoj osobi.

Pristup sa eksternih lokacija mora biti kontrolirano i omogućeno isključivo preko zatvorenih sigurnosnih tunela ili VPN tunela

Svaki pristup Informacionom sistemu mora biti automatski zabilježen jedinstvenim identifikatorom osobe u bazi podataka Jedinstvenog sistema te tačnim vremenom pristupa.

Svaki pokušaj neovlaštenog pristupa Informacionom sistemu mora biti automatski zabilježen datumom, vremenom, mjestom sa kojeg je takav pristup pokušan i jedinstvenim identifikatorom osobe koja je pokušala pristupiti.

Administratori baze podataka Jedinstvenog sistema su dužni na mjesečnoj osnovi i u pisanom obliku obavještavati rukovodioca Službe za finansije o svim pokušajima neovlaštenog pristupa.

Član 7.

Sistem administrator ili drugo ovlašteno lice upravlja korisničkim računima, pravima pristupa i korisničkim lozinkama za interne i eksterne korisnike baze podataka Jedinstvenog sistema.

Svaki korisnik sistema ima jedinstveno korisničko ime i korisničku lozinku. Korisnička lozinka se mora sastojati od najmanje _____ karaktera i sadržavati specijalni znak _____.

Korisnici baze podataka Jedinstvenog sistema su dužni:

a) dodijeljenu korisničku lozinku korisnici su dužni _____ mijenjati, na način da podnesu zahtjev za promjenu lozinke administratoru,
b) koristiti prijavu tako da neovlašteni zaposlenici i druga lica ne mogu doći u priliku da je saznaju,
c) koristiti prijavu i informacije tako da u potpunosti štite podatke dostupne putem računara i terminala i
d) spriječiti i na vrijeme informisati neposrednog rukovodioca o svim pokušajima neovlaštenih zaposlenika ili drugih lica da saznaju prijavu za koju nisu ovlašteni.

Član 8.

Prijava, zajedno sa korisničkim imenom i šifrom, jednoznačno određuje verifikaciju i

autorizaciju korisnika.

Zahtjev sa spiskom lica kojima treba otvoriti prijavu, odnosno dodijeliti odgovarajuće korisničko ime i korisničku lozinku, podnosi nadležni rukovodilac organizacionog dijela iz kojeg dolazi korisnik. Zahtjev se podnosi sistemu administratoru, na propisanom obrascu koji čini sastavni dio ovog Pravilnika.

Po primljenom zahtjevu, sistem administrator ili drugo ovlašteno lice je dužno odmah postupiti. Prijava se dostavlja podnosiocu zahtjeva u zatvorenoj koverti.

Ovlaštenje za prijavu, odnosno pristup podacima drugog organizacionog dijela, može se dati samo uz pismenu saglasnost neposrednog rukovodioca tog organizacionog dijela. Uvid u sve otvorene prijave na sistemu imaju samo sistem administratori ili ovlaštena lica.

Podaci o pravima pristupa se trebaju čuvati na sigurnom mjestu, po mogućnosti u sefu sa vatrootpornom zaštitom.

(Trag aktivnosti/promjena)

Član 9.

Aplikativni sistem treba da obezbijedi evidentiranje aktivnosti svih korisnika/operatera u sistemu: operater koji je aktivirao servis, vrstu servisa koji je korišten, podatke sa kojima je rađeno (pregled/modifikacija) sa tragom promjena (stari podatak - ako postoji, novi podatak), datum i vrijeme promjene, lokacija i terminal sa kojeg je izvršena promjena/uvid u podatke.

Sistem treba da ima mogućnost da na osnovu ovih podataka izvrši restauraciju stanja do željenog vremenskog trenutka (za koji postoji sačuvan trag promjena).

Pored praćenja promjena podataka u aplikativnom sistemu, za svaki podsistem definišu se informacije koje operativni sistem pamti u istorijski (log) fajl, kao npr.:

a) Informacije o prijavi na sistem (Logon/logoff information),
b) Informacije o isključenju/uključenju sistema
c) Pristup datotekama i direktorijumima
d) Promjene korisničkih šifri
e) Pristup sistemskim objektima
f) Promjene sigurnosnih ''politika'' ugranenih u sistem (policy changes) itd.

(Mjere zaštite i sigurnosti podataka Jedinstvenog sistema)

Član 10.

Općinska uprava je obavezna zaštititi bazu podataka Jedinstvenog sistema od internih i eksternih opasnosti.

Obezbijediti da sistem bude zatvorenog tipa uz kontrolisan pritup vanjskim mrežnim reusrsima kao i zabranu svih dolaznih konekcija osim onih koje imaju validnu dozvolu od strane sistem administratora ili drugog ovlaštenog lica

Sistem administrator ili drugo ovlašteno lice je dužno instalirati i održavati legalni komercijalni softver za zaštitu baze podataka Jedinstvenog sistema i ostalih baza podataka općinske uprave od virusa i ostalih malicioznih kodova.

Član 11.

Mrežna sigurnost se implementira kako bi se rizik od internih i eksternih opasnosti za bazu podataka Jedinstvenog sistema sveo na minimum.

Potrebno je osigurati prenos podataka Jedinstvenog sistema dislociranim korisnicima Jedinstvenog sistema, kako bi se spriječio gubitak ili krađa podataka Jedinstvenog sistema.

Član 12.

O svim sigurnosnim incidentima u bazi podataka Jedinstvenog sistema, odmah i u pisanom obliku mora se obavijestiti nadležni rukovodilac organizacionog dijela ili direktno Sistem administratora.

Član 13.

Dogradnja sistema zaštite vršiće se kontinuirano, u skladu sa rezultatima procjene sigurnosti sistema, praktičnim iskustvima narušavanja sigurnosti ili pokušaja za narušavanje sigurnosti sistema, razvojem tehnologija, organizacionih i funkcionalnih promjena, kao i svih drugih aspekata koji imaju uticaj na sigurnost sistema.

Za sigurnost sistema odgovoran je sistem administrator ili drugo ovlašteno lice.

Na godišnjem osnovu, Administrator sačinjava izvještaj kojim ocjenjuje čuvanje i sigurnost podataka Jedinstvenog sistema, daje prijedloge vezano za korektivne mjere i usklađivanje postupaka i mjera koji su neophodni za kontinuitet baze podataka Jedinstvenog sistema i daje preporuke radi unapređenja sigurnosti, pohranjivanja i zaštite podataka Jedinstvenog sistema.

(Fizička zaštita i rekonstrukcija baze podataka Jedinstvenog sistema)

Član 14.

Centralna lokacija operacija baze podataka Jedinstvenog sistema, druge dislocirane lokacije baze podataka Jedinstvenog sistema i lokacija za pohranjivanje sigurnosnih kopija moraju biti na adekvatan način zaštićene od požara i drugih neplaniranih događaja, te imati 24-satni sigurnosni sistem.

Lokacija za pohranjivanje sigurnosnih kopija se treba nalaziti izvan centralne lokacije operacija baze podataka Jedinstvenog sistema, koja se nalazi _____.

Član 15.

Za slučaj gubitka, oštećenja ili uništenja podataka unesenih u Jedinstveni sistem, izrađuje se sigurnosna kopija, na način da se podaci uneseni u Jedinstveni sistem prenose na prenosive informatičke medije.

Minimalni zahtjevi za pohranjivanje podataka su:

1. noćno pohranjivanje potpunih podataka na prenosive informatičke medije i
2. sedmično pohranjivanje potpunih podataka na prenosive informatičke medije koje se provodi posljednji radni dan u sedmici.

Sigurnosne kopije podataka Jedinstvenog sistema na prenosivim medijima moraju se čuvati na odgovarajućem mjestu.

Podaci se moraju čuvati na sigurnom mjestu, sa kontrolom pristupa, uz adekvatan način zaštite od požara i drugih neplaniranih događaja. Pristup lokaciji i opremi mora biti fizički zaštićen i dozvoljen samo ovlaštenim osobama.

Član 16.

Najmanje jednom sedmično, potrebno je testirati mogućnost povrata podataka sa sigurnosnih kopija.

Najmanje jednim godišnje mora se vršiti potpuni povrat pohranjenih podataka sa sigurnosnih kopija podataka Jedinstvenog sistema radi testiranja procesa, opreme i medija za pohranjivanje.

(Održavanje, popravak i povlačenje iz upotrebe opreme za Jedinstveni sistem)

Član 17.

Obaveza je osigurati održavanje računarske opreme za Jedinstveni sistem.

Prije popravljanja, moraju se spremiti sigurnosne kopije podataka koji se nalaze na računarskoj opremi za Jedinstveni sistem kako bi se spriječio gubitak podataka.

Član 18.

Zaposlenici vanjskih kompanija koje vrše održavanje i popravke opreme, prilikom svakog pristupa lokacijama operacija baze podataka Jedinstvenog sistema i čuvanja sigurnosnih kopija, moraju biti pod nadzorom ovlaštenih zaposlenika Općine.

Svi zaposlenici vanjskih kompanija koji bi prilikom održavanja i popravljanja mogli imati pristup bazi podataka Jedinstvenog sistema su dužni potpisati izjave o sigurnosti podataka.

Član 19.

Nakon povlačenja iz upotrebe računarske opreme za Jedinstveni sistem, svi podaci Jedinstvenog sistema, memorisani na radnu memoriju i tvrde diskove moraju biti sigurno i trajno sačuvani izbrisani.

(Prelazne i završne odredbe)

Član 20.

U skladu sa odredbama ovog Pravilnika, načelnik općine i/ili rukovodilac organizacione jedinice donosi odluke kojima određuje poslove i dužnosti Sistem administratora i drugih ovlaštenih lica za čuvanje i sigurnost podataka i Jedinstvenog sistema u cjelini i određuje poslove, dužnosti i način rada korisnika sistema na Jedinstvenom sistemu.

Član 21.

Ovaj pravilnik stupa na snagu danom donošenja, a bit će objavljen u Sl. glasniku Općine.

OPĆINSKI NAČELNIK