Bosna i Hercegovina
BRČKO DISTRIKT
BOSNE I HERCEGOVINE
DIREKCIJA ZA
FINANSIJE/FINANCIJE

Босна и Херцеговина
Б Р Ч К О Д И С Т Р И К Т БОСНЕ
И ХЕРЦЕГОВИНЕ
ДИРЕКЦИЈА ЗА
ФИНАНСИЈЕ/ФИНАНЦИЈЕ

Міирослава Крлеже1, 76100 Брчко Дистрикт Босне и Херцеговине; Телефон: 049/ 220 890, Факс: 049/ 212 984,
IMroslava Krleže 1, 76100 Brčko Distrikt Bosne i Hercegovine; Telefon: 049/ 220 890, Факс: 049/ 212 984,

Broj:_____
Brčko,07.09.2007. godine

Na osnovu člana 12. stav 1. tačka c. Zakona o Direkciji za finansije ("Službeni glasnik Brčko distrikta BiH", broj: 19/07) , člana 21. stav 4. i člana 33. stav 1. tačka g) Zakona o Trezoru Brčko distrikta BIH ("Službenik glasnik Brčko distrikta BiH", broj: 3/07, 19/07), Direktor Direkcije za finansije Brčko distrikta BiH donosi:

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

OPŠTE ODREDBE I

ČLAN 1

Ovim Pravilnikom se uređuje informatička i funkcionalna zaštita računovodstvenog sistema glavne knjige Trezora i pomoćnih knjiga, prijem i obrada, zaštita i distribucija obrađenih podataka, u uslovima računarske obrade podataka.

ČLAN 2.

(1) Razmjena podataka (prijem i slanje) između korisnika vrši se modemski ili elektronskom poštom.

(2) Evidencije o razmijenjenim podacima čuvaju se u elektronskoj formi.

Član 3.

(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 institucije ili od njega ovlaštenog lica.

Član 4.

Za sve podatke na memorijskim medijima sprovodi se zaštita u skladu sa uputstvom_za zaštitu podataka.

ČLAN 5.

(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.

ZAŠTITA TAJNOSTI PODATAKA NA RAČUNARSKOJ MREŽI II

Član 6.

(1)U ovom poglavlju regulisane su nadležnosti, prava i obaveze u pogledu:

a) prava pristupa i raspolaganja informacijama i podacima koji se mogu se dobiti u radu na računarskoj mreži,

b) nadležnosti u pogledu zahtjeva za dodjelu i izmjenu prijava kao i njegove realizacije i distribucije,

c) ostala pitanja iz ove oblasti.

(2) Pravilima zaštite u smislu ovog Pravilnika podliježu podaci koje koriste programska rješenja, odnosno podaci o poslovanju organa i institucija Brčko distrikta, u skladu sa pozitivnim zakonskim odredbama.

(3) Pristup podacima iz prethodnog stava imaju zaposlenici koji neposredno rade na računarima kao i drugi zaposlenici , po posebnom ovlaštenju rukovodioca organizacione jedinice/cijeline.

(4) Korištenje podataka vrši se putem odgovarajuće prijave (login-a i password-a) koja se otvara i na sistemu i na relacionoj bazi.

(5) Passwordi se postavljaju na način:

a) da je dužina najmanje 6 znakova,
b) da se moraju mijenjati najmanje svakih 6 mjeseci,
c) da se čuva istorija njihovih promjena,
d) da se korisnicima onemogući daljnji pristup sistemu nakon tri neuspjela pokušaja,
e) da se neuspjeli pokušaji pristupa sistemu zapisuju u datoteku (log file) i
f) da se zahtijeva kompletna struktura passworda.

Član 7.

(1) Prijava, zajedno sa korisničkim imenom i šifrom, jednoznačno određuje verifikaciju i autorizaciju korisnika.

(2) Zahtjev sa spiskom lica kojima treba otvoriti prijavu, odnosno dodijeliti odgovarajući login i password, podnosi nadležni rukovodilac organizacionog dijela u kojem se posao obavlja. Zahtjev se podnosi sistemu administratoru, na propisanom obrascu koji čini sastavni dio ovog Pravilnika.

(3) Po primljenom zahtjevu, sistem administrator ili drugo ovlašteno lice je dužno odmah postupiti.

(4) Ovlaštenje za prijavu, odnosno pristup podacima drugog organizacionog dijela, može se dati samo uz pismenu saglasnost neposrednog rukovodioca tog organizacionog dijela.

Član 8.

(1) U slučaju da se podnosilac zahtjeva i sistem administrator ne mogu usaglasiti u pogledu ovlaštenja za pristup podacima, odluku o tome donosi rukovodilac organizacione jedinice/cijeline.

(2) Po prestanku potrebe za rad koji je omogućavala, prijava se mora ukinuti, a na osnovu zahtjeva nadležnog rukovodioca.

(3) Prijava se mora mijenjati ukoliko se sazna da je neovlašteno lice došlo u poziciju da je sazna.

(4) Ovlašteni zaposlenik koji raspolaže prijavom dužan je:

a) dodijeljeni password u okviru tek otvorene prijave odmah promijeniti, a u cilju zaštite i povremeno mijenjati,

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 9.

(1) Prijavu na računarskom sistemu ažurira isključivo sistem administrator ili ovlašteno lice, na osnovu pismenog zahtjeva iz člana 7. ovog Pravilnika.

(2) Prijava se dostavlja podnosiocu zahtjeva u zatvorenoj koverti.

(3) Uvid u sve otvorene prijave na sistemu imaju samo sistem administratori ili ovlaštena lica.

(4) Nije dozvoljeno formirati, kopirati ili distribuirati spisak otvorenih prijava, bez odobrenja direktora ili od njega ovlaštenog lica.

Član 10.

(1) Ako liste i izvještaje preuzima zaposlenik koji nije ovlašten, lista se mora predavati u zatvorenoj koverti.

(2) Za podatke koji su predmet zaštite, u smislu ovog Pravilnika, se vodi poseban registar koji sadržava:

a) redni broj i datum,
b) ime i prezime zaposlenika koji je dao nalog za izradu liste i izvještaja,
c) datum izrade liste i izvještaja,
d) ime, prezime i potpis zaposlenika koji je listu i izvještaj izradio,
e) ime, prezime i potpis zaposlenika koji je listu i izvještaj preuzeo.

Član 11.

Puna zaštita (backup) za sve serverske mašine radi se obavezno jednom godišnje software-om za full-backup serverskih mašina, a po potrebi i češće (ukoliko je bilo izmjena u operativnom sistemu, dodavanja novih patch-eva, file-system-a i slično).

Član 12.

(1) Podaci, odnosno tablice, iz baza podataka štite se svakodnevno na kraju radnog dana ili po potrebi
(2) Aplikacije (programi) iz baza štite se prilikom instalacije, ili svake izmjene i dopune softvera i obavezno na kraju fiskalne godine.
(3) Nakon završetka poslovne godine rade se trajne godišnje zaštite na CD-u/DVD-u u dvije kopije.

(4) DNS-serveri **-** Kompletan direktorij štiti se na lokalni disk u slučaju izmjena.
(5) WINDOWS 2000 serveri - Direktorij sa SQL/Access/Excel programima štiti se na disk i CD/DVD prema potrebi, ukoliko je bilo izmjena na programima.
(6) WINDOWS 2003 serveri - Na kraju svake kalendarske godine radi se zaštita svih datoteka u kriptovanom i enkriptovanom formatu na CD-u (2 kopije) i trajno se pohranjuje.
(7) Kopije trajnih godišnjih zaštita čuvaju se na predviđenoj lokaciji za arhivu.
(8) Provjera tehničke ispravnosti medija - Na kraju svake kalendarske godine, nakon završenih godišnjih arhiviranja radi se pregled arhiviranih podataka, a najkasnije do 31.03. tekuće godine.

ZAŠTITA MAGNETNIH MEDIJA III

Član 13.

(1) Pod magnetnim medijima u smislu ovog Pravilnika se podrazumijevaju: magnetne trake, floppy diskete, CD diskete i ZIP diskete.

(2) Mjesta na kojima se mediji arhiviraju su:

a) arhiva magnetnih medija u sistem sali,
b) vatrostalni ormar,
c) ormar za magnetne medije,
d) udaljena sigurna lokacija za čuvanje backup-a.

(3) Ostala mjesta se smatraju privremenim.

(4) Mediji se mogu, po nalogu nadležnog lica, odlagati i na drugim mjestima (arhiva, trezor i sl.).

(5) Podaci na svim medijima moraju se osvježavati (čitati i presnimavati) .

Član 14.

(1) Zabranjeno je umnožavanje, presnimavanje i publikovanje magnetnih medija.

(2) Ako se određena oprema stavlja van upotrebe, potrebno je obezbijediti prepis podataka sa dotadašnjih medija u novi oblik (konverzija, štampa, snimak itd.).

Član 15.

(1) Svaka magnetna traka mora imati jedinstvenu oznaku. Oznaka je sastavljena po šemi:

a) N- yyyymmdd -B – pri čemu oznaka:
b) N- predstavlja naziv npr. BAZA;
c) yyyymmdd: predstavlja datum;
d) B- predstavlja broj blokova.

(2) Naljepnica sa oznakom mora biti na samoj traci.

(3) Podaci na trakama se vode u registru, koji sadrži slijedeće podatke:

a) oznaka trake – broj,
b) datum rada,
c) opis sadržaja.

(4) Trake koje se čuvaju duže od jedne godine oslobađaju se ako se za to dobije saglasnost sistem administratora i rukovodioca organizacionog dijela čiji se podaci štite.

(5) Rokovi i broj generacija zaštita za svaku pojedinu grupu poslova odrediti će se uputstvom.

(6) Broj generacija zaštite u arhivi po potrebi može propisati sistem administrator, ovlašteno lice ili nadležni rukovodilac.

Član 16.

(1) Preuzimanje trake od strane ovlaštenih radnika se vrši uz evidenciju o primopredaji. U evidenciji se obavezno navode slijedeći podaci:

a) datum preuzimanja,

b) ime i prezime lica koje je preuzelo traku,
c) datum vraćanja.

(2) Oštećene trake se izdvajaju i vidno obilježavaju. Uništavanje oštećenih traka se vrši zapisnički. Zapisnik sastavljaju:

a) sistem administrator;
b) samostalni referent za poslove obrade;
c) referent koji vrši evidenciju opreme.

(3) U zapisniku se navode:

a) oznake uništenih traka;
b) datum uništenja;
c) mjesto i način uništavanja.

Član 17.

(1) Svaki medij mora imati oznaku na kojoj su navedeni podaci o sadržaju.

(2) Za izvorne programe mora biti navedeno:

a) tačan naziv aplikacije;
b) datum;
c) redni broj bloka (po potrebi)

(3) Svaki uređaj na kojima se štite podaci mora imati oznaku sa slijedećim podacima:

a) aplikacija, odnosno grupa poslova,
b) datum zaštite i
c) datum ažurnosti..

(4) Za ostale korisnike, koji posao obavljaju na personalnom računaru, propisuje se isti način zaštite podataka na disketama. Korisnici su sami dužni napraviti i čuvati ovu zaštitu u slučaju da hardwerski strada disk i na taj način im propadnu podaci (razne vrste korisničkih izvještaja).

(5) Po isteku roka čuvanja podataka na medijima potrebno je nepovratno izbrisati sadržaj medija.

PREVENTIVNE MJERE IV

Član 18.

(1) Proaktivne mjere podrazumjevaju moguće rizične situacije i atake na sistemske resurse i definišu mjere kojima se eliminiše/minimizuje mogućnost realizacije napada ili posljedice omaški/nenamjernih grešaka.

(2) Ove mjere se odnose na fizičke i ne-fizičke mjere zaštite podataka koje su definisane u sledećim poglavljima.

A. ''Ne-fizičke'' mjere zaštite podataka

Član 19.

(1) Ovim mjerama zaštite određuju se smjernice za aktivnosti koje je moguće izvršiti odgovarajućim postavkama informacionog sistema na svim nivoima (od najnižeg fizičkog nivoa do najvišeg logičkog - aplikativnog nivoa).

(2)Pravima pristupa su definisani servisi/funkcije koji su na raspolaganju vlasniku prava, licencirane lokacije sa kojih se ti servisi mogu koristiti, te naznačen opseg podataka sa kojim može da radi vlasnik odnosnog prava prilikom korištenja odnosnog servisa.

(3) Za implementaciju ovih mjera zaštite sistema odgovorne su kompanije ili organizacione jedinice koje su kreirale sistem.

B. Trag aktivnosti/promjena

Član 20.

(1) 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.

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

(3)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 (System shutdown and restart information)
c) Pristup datotekama i direktorijumima
d) Promjene korisničkih šifri
e) Pristup sistemskim objektima
f) Promjene sigurnosnih ''politika'' ugrađenih u sistem (policy changes) itd.

C. Pravila za dodjeljivanje i korištenje korisničkih i administratorskih šifri (password-a) i autentifikaciju

Član 21.

(1) Glavne/supervizorske administratorske šifre (BIOS-a, operativnog sistema, baze podataka i slično) treba da budu deponovane u zapečaćenim kovertama na, za to određeno posebno mjesto.

(2) Procedure za dodjelu, promjenu, deponovanje i kontrolu šifara glavnih administratora treba da budu specificirane za svaki server i bazu podataka.

(3) Korisničke šifre moraju biti dužine 6-8 karaktera, uključivati velika i mala slova i brojeve (opciono i kontrolne karaktere). Pasword ne smije uključivati identifikator korisnika (login name), imena/prezimena članova porodice u normalnom ili invertovanom redoslijedu).

a) Korisničke šifre se moraju mijenjati periodično.
b) Korisnici moraju pamtiti svoje korisničke šifre (ne smiju ih imati zapisane).
c) Korisnička šifra mora biti specificirana u procesu autentifikacije korisnika.
d) Korisnici ne smiju otkrivati svoju korisničku šifru nikome (uključujući administratore).
e) Inicijalno dodijeljena korisnička šifra od strane administratora, mora biti promijenjena od strane korisnika odmah nakon prvog prijavljivanja.
f) Korisnik treba da ima mogućnost promjene svoje korisničke šifre bez intervencije nadležnog administratora.
g) Transfer korisničkih šifara kroz komunikacionu mrežu mora biti zaštićen od mogućnosti presretanja na mreži i otkrivanja.

D. Dogradnja sistema zaštite

Član 22.

(1) 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.

(2) Za sigurnost sistema odgovoran je sistem administrator.

E. Fizičke mjere zaštite

Član 23.

Za svaku organizacionu jedinicu potrebno je definisati:

a) Pravila pristupa i kretanja u prostorijama za zaposlene i eksterni personal ,
b) Pravila zaštite mašinski čitljivih podataka i štampanog materijala,
c) Ograničenja u kopiranju podataka,
d) Pravila transportovanja podataka i dokumenata,
e) Pravila korištenja telefona, faksova, digitalnih kamera itd.,
f) Ostale mjere zaštite (od požara, poplava, gubitka napajanja električnom energijom i slično).

KONZERVATIVNE MJERE ZAŠTITE PODATAKA V

Član 24.

Konzervativne mjere se primjenjuju za slučaj da se dogodio kvar ili napad na sistem, i tada treba primijeniti slijedeće korake:

a) Procijeniti štetu,
b) Utvrditi uzrok i razlog problema/havarije,
c) Otkloniti kvar/grešku i (ili) posljedice havarije/napada (primijeniti pravila politike i kontrole mjere sigurnosti),
d) Dokumentovati događaj i primijenjene postupke, izvući zaključke i po potrebi ažurirati plan sigurnosti i uvesti dodatne mjere i postupke,
e) Eventualno primijeniti alternativni plan kako bi se obezbijedio kontinuitet aktivnosti sistema.

PRELAZNE I ZAVRŠNE ODREDBE VII

Član 25.

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

Direktor,
Mato Lučić, dipl.ecc