

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



**Босна и Херцеговина
БРЧКО ДИСТРИКТ БОСНЕ
И ХЕРЦЕГОВИНЕ
ДИРЕКЦИЈА ЗА
ФИНАНСИЈЕ/ФИНАНСИЈЕ**

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

Број: _____
Брчко, 07.09.2007. године

На основу члана 12. став 1. тачка ц. Закона о Дирекцији за финансије ("Службени гласник Брчко дистрикта БиХ", број: 19/07), члана 21. став 4. и члана 33. став 1. тачка г) Закона о Трезору Брчко дистрикта БИХ ("Службеник гласник Брчко дистрикта БиХ", број: 3/07, 19/07), Директор Дирекције за финансије Брчко дистрикта БиХ доноси:

П Р А В И Л Н И К О ИНФОРМАТИЧКОЈ И ФУНКЦИОНАЛНОЈ ЗАШТИТИ РАЧУНОВОДСТВЕНОГ СИСТЕМА ГЛАВНЕ КЊИГЕ ТРЕЗОРА И ПОМОЋНИХ КЊИГА МОДУЛА

ОПШТЕ ОДРЕДБЕ I

Члан 1

Овим Правилником се уређује информатичка и функционална заштита рачуноводственог система главне књиге Трезора и помоћних књига, пријем и обрада, заштита и дистрибуција обрађених података, у условима рачунарске обраде података.

Члан 2.

(1) Размјена података (пријем и слање) између корисника врши се модемски или електронском поштом.

(2) Евиденције о размијењеним подацима чувају се у електронској форми.

Члан 3.

(1) Обрада и динамика обраде података се обављају према позитивним законским прописима и стандардима из области рачуноводства.

(2) Промјена динамике обраде врши се уз сагласност руководиоца органа или институције или од њега овлашћеног лица.

Члан 4.

За све податке на меморијским медијима спроводи се заштита у складу са упутством_за заштиту података.

ЧЛАН 5.

(1) Након завршене обраде, листе и извјештаји предвиђени апликацијама се штампају прописаном динамиком и у прописаном обиму. Штампани материјал се разврстава по врстама и корисницима након чега се дистрибуира корисницима.

(2) По претходно прибављеној сагласности руководиоца органа или институције или од њега овлаштеног лица у складу са позитивним законским прописима из области рачуноводства, утврђују се начин и рокови дистрибуције штампаног материјала.

(3) Штампани извјештаји или датотеке из архиве достављају се корисницима, у складу са одговарајућим налогом, уз потврду пријема.

ЗАШТИТА ТАЈНОСТИ ПОДАТАКА НА РАЧУНАРСКОЈ МРЕЖИ II

Члан 6.

(1) У овом поглављу регулисане су надлежности, права и обавезе у погледу:

- a) права приступа и располагања информацијама и подацима који се могу се добити у раду на рачунарској мрежи,
- b) надлежности у погледу захтјева за додјелу и измјену пријава као и његове реализације и дистрибуције,
- c) остала питања из ове области.

(2) Правилима заштите у смислу овог Правилника подлијежу подаци које користе програмска рјешења, односно подаци о пословању органа и институција Брчко дистрикта, у складу са позитивним законским одредбама.

(3) Приступ подацима из претходног става имају запосленици који непосредно раде на рачунарима као и други запосленици, по посебном овлаштењу руководиоца организационе јединице/цијелине.

(4) Кориштење података врши се путем одговарајуће пријаве (логин-а и пасворд-а) која се отвара и на систему и на релационој бази.

(5) Пасворди се постављају на начин:

- a) да је дужина најмање 6 знакова,
- b) да се морају мијењати најмање сваких 6 мјесеци,
- c) да се чува историја њихових промјена,
- d) да се корисницима онемогући даљњи приступ систему након три неуспјела покушаја,
- e) да се неуспјели покушаји приступа систему записују у датотеку (лог филе) и
- f) да се захтјева комплетна структура пасворда.

Члан 7.

(1) Пријава, заједно са корисничким именом и шифром, једнозначно одређује верификацију и ауторизацију корисника.

(2) Захтјев са списком лица којима треба отворити пријаву, односно додијелити одговарајући логин и пасворд, подноси надлежни руководилац организационог дијела у којем се посао обавља. Захтјев се подноси систему администратору, на прописаном обрасцу који чини саставни дио овог Правилника.

(3) По примљеном захтјеву, систем администратор или друго овлаштено лице је дужно одмах поступити.

(4) Овлаштење за пријаву, односно приступ подацима другог организационог дијела, може се дати само уз писмену сагласност непосредног руководиоца тог организационог дијела.

Члан 8.

(1) У случају да се подносилац захтјева и систем администратор не могу усагласити у погледу овлаштења за приступ подацима, одлуку о томе доноси руководилац организационе јединице/цијелине.

(2) По престанку потребе за рад који је омогућавала, пријава се мора укинути, а на основу захтјева надлежног руководиоца.

(3) Пријава се мора мијењати уколико се сазна да је неовлаштено лице дошло у позицију да је сазна.

(4) Овлаштени запосленик који располаже пријавом дужан је:

- a) додијељени пасворд у оквиру тек отворене пријаве одмах промијенити, а у циљу заштите и повремено мијењати,
- b) користити пријаву тако да неовлаштени запосленици и друга лица не могу доћи у прилику да је сазнају,
- c) користити пријаву и информације тако да у потпуности штите податке доступне путем рачунара и терминала и
- d) спријечити и на вријеме информисати непосредног руководиоца о свим покушајима неовлашћених запосленика или других лица да сазнају пријаву за коју нису овлаштени.

Члан 9.

(1) Пријаву на рачунарском систему ажурира искључиво систем администратор или овлаштено лице, на основу писмог захтјева из члана 7. овог Правилника.

(2) Пријава се доставља подносиоцу захтјева у затвореној коверти.

(3) Увид у све отворене пријаве на систему имају само систем администратори или овлаштена лица.

(4) Није дозвољено формирати, копирати или дистрибуирати списак отворених пријава, без одобрења директора или од њега овлашћеног лица.

Члан 10.

(1) Ако листе и извјештаје преузима запосленик који није овлашћен, листа се мора предавати у затвореној коверти.

(2) За податке који су предмет заштите, у смислу овог Правилника, се води посебан регистар који садржава:

- a) редни број и датум,
- b) име и презиме запосленика који је дао налог за израду листе и извјештаја,
- c) датум израде листе и извјештаја,
- d) име, презиме и потпис запосленика који је листу и извјештај израдио,
- e) име, презиме и потпис запосленика који је листу и извјештај преузео.

Члан 11.

Пуна заштита (бацкуп) за све серверске машине ради се обавезно једном годишње софтвере-ом за фулл-бацкуп серверских машина, а по потреби и чешће (уколико је било измјена у оперативном систему, додавања нових патцх-ева, филе-систем-а и слично).

Члан 12.

- (1) Подаци, односно таблице, из база података штите се свакодневно на крају радног дана или по потреби
- (2) Апликације (програми) из база штите се приликом инсталације, или сваке измјене и допуне софтвера и обавезно на крају фискалне године.
- (3) Након завршетка пословне године раде се трајне годишње заштите на ЦД-у/ДВД-у у двије копије.
- (4) ДНС-сервери - Комплетан директориј штити се на локални диск у случају измјена.
- (5) WINDOWS 2000 сервери - Директориј са СQL/Аццесс/Ехцел програмима штити се на диск и ЦД/ДВД према потреби, уколико је било измјена на програмима.
- (6) WINDOWS 2003 сервери - На крају сваке календарске године ради се заштита свих датотека у криптованом и енкриптованом формату на ЦД-у (2 копије) и трајно се похрањује.
- (7) Копије трајних годишњих заштита чувају се на предвиђеној локацији за архиву.
- (8) Провјера техничке исправности медија - На крају сваке календарске године, након завршених годишњих архивирања ради се преглед архивираних података, а најкасније до 31.03. текуће године.

ЗАШТИТА МАГНЕТНИХ МЕДИЈА III

Члан 13.

- (1) Под магнетним медијима у смислу овог Правилника се подразумевају: магнетне траке, флоппу дискете, ЦД дискете и ЗИП дискете.
- (2) Мјеста на којима се медији архивирају су:
 - a) архива магнетних медија у систем сали,
 - b) ватростални ормар,
 - c) ормар за магнетне медије,
 - d) удаљена сигурна локација за чување бацкуп-а.
- (3) Остала мјеста се сматрају привременим.
- (4) Медији се могу, по налогу надлежног лица, одлагати и на другим мјестима (архива, трезор и сл.).
- (5) Подаци на свим медијима морају се освјежавати (читати и преснимавати) .

Члан 14.

- (1) Забрањено је умножавање, преснимавање и публиковање магнетних медија.
- (2) Ако се одређена опрема ставља ван употребе, потребно је обезбиједити препис података са дотадашњих медија у нови облик (конверзија, штампа, снимак итд.).

Члан 15.

- (1) Свака магнетна трака мора имати јединствену ознаку. Ознака је састављена по шеми:
 - a) Н- ууууммдд -Б – при чему ознака:
 - b) Н- представља назив нпр. БАЗА;
 - c) ууууммдд: представља датум;
 - d) Б- представља број блокова.
- (2) Наљепница са ознаком мора бити на самој траци.
- (3) Подаци на тракама се воде у регистру, који садржи слиједеће податке:
 - a) ознака траке – број,
 - b) датум рада,
 - c) опис садржаја.

(4) Траке које се чувају дуже од једне године ослобађају се ако се за то добије сагласност систем администратора и руководиоца организационог дијела чији се подаци штите.

(5) Рокови и број генерација заштита за сваку поједину групу послова одредити ће се упутством.

(6) Број генерација заштите у архиви по потреби може прописати систем администратор, овлаштено лице или надлежни руководиоца.

Члан 16.

(1) Преузимање траке од стране овлашћених радника се врши уз евиденцију о примопредаји. У евиденцији се обавезно наводе слиједећи подаци:

- a) датум преузимања,
- b) име и презиме лица које је преузело траку,
- c) датум враћања.

(2) Оштећене траке се издвајају и видно обиљежавају. Уништавање оштећених трака се врши записнички. Записник састављају:

- a) систем администратор;
- b) самостални референт за послове обраде;
- c) референт који врши евиденцију опреме.

(3) У записнику се наводе:

- a) ознаке уништених трака;
- b) датум уништења;
- c) мјесто и начин уништавања.

Члан 17.

(1) Сваки медиј мора имати ознаку на којој су наведени подаци о садржају.

(2) За изворне програме мора бити наведено:

- a) тачан назив апликације;
- b) датум;
- c) редни број блока (по потреби)

(3) Сваки уређај на којима се штите подаци мора имати ознаку са слиједећим подацима:

- a) апликација, односно група послова,
- b) датум заштите и
- c) датум ажурности..

(4) За остале кориснике, који посао обављају на персоналном рачунару, прописује се исти начин заштите података на дискетама. Корисници су сами дужни направити и чувати ову заштиту у случају да хардверски страда диск и на тај начин им пропадну подаци (разне врсте корисничких извјештаја).

(5) По истеку рока чувања података на медијима потребно је неповратно избрисати садржај медија.

ПРЕВЕНТИВНЕ МЈЕРЕ IV

Члан 18.

(1) Проактивне мјере подразумјевају могуће ризичне ситуације и атакe на системске ресурсе и дефинишу мјере којима се елиминише/минимизује могућност реализације напада или посљедице омашки/ненамјерних грешака.

(2) Ове мјере се односе на физичке и не-физичке мјере заштите података које су дефинисане у следећим поглављима.

A. "Не-физичке" мјере заштите података

Члан 19.

(1) Овим мјерама заштите одређују се смјернице за активности које је могуће извршити одговарајућим поставкама информационог система на свим нивоима (од најнижег физичког нивоа до највишег логичког - апликативног нивоа).

(2) Правима приступа су дефинисани сервиси/функције који су на располагању власнику права, лиценциране локације са којих се ти сервиси могу користити, те назначен опсег података са којим може да ради власник односног права приликом кориштења односног сервиса.

(3) За имплементацију ових мјера заштите система одговорне су компаније или организационе јединице које су креирале систем.

Б. Траг активности/промјена

Члан 20.

(1) Апликативни систем треба да обезбиди евидентирање активности свих корисника/оператера у систему: оператер који је активирао сервис, врсту сервиса који је кориштен, податке са којима је рађено (преглед/модификација) са трагом промјена (стари податак - ако постоји, нови податак), датум и вријеме промјене, локација и терминал са којег је извршена промјена/увид у податке.

(2) Систем треба да има могућност да на основу ових података изврши рестаурацију стања до жељеног временског тренутка (за који постоји сачуван траг промјена).

(3) Поред праћења промјена података у апликативном систему, за сваки подсистем дефинишу се информације које оперативни систем памти у историјски (лог) фајл, као нпр.:

- a) Информације о пријави на систем (Логон/логофф информатион),
- b) Информације о искључењу/укључењу система (Сустем схутдаун анд рестарт информатион)
- c) Приступ датотекама и директоријумима
- d) Промјене корисничких шифри
- e) Приступ системским објектима
- f) Промјене сигурносних "политика" уграђених у систем (полицу цхангес) итд.

Ц. Правила за додјељивање и кориштење корисничких и администраторских шифри (пасворд-а) и аутентификацију

Члан 21.

(1) Главне/супервизорске администраторске шифре (БИОС-а, оперативног система, базе података и слично) треба да буду депоноване у запечаћеним ковертама на, за то одређено посебно мјесто.

(2) Процедуре за додјелу, промјену, депоновање и контролу шифара главних администратора треба да буду специфициране за сваки сервер и базу података.

(3) Корисничке шифре морају бити дужине 6-8 карактера, укључивати велика и мала слова и бројеве (опционо и контролне карактере). Пасворд не смије укључивати идентификатор корисника (логин наме), имена/презимена чланова породице у нормалном или инвертованом редослиједу).

- a) Корисничке шифре се морају мијењати периодично.
- b) Корисници морају памтити своје корисничке шифре (не смију их имати записане).
- c) Корисничка шифра мора бити специфицирана у процесу аутентификације корисника.
- d) Корисници не смију откривати своју корисничку шифру никоме (укључујући администраторе).
- e) Иницијално додијељена корисничка шифра од стране администратора, мора бити промијењена од стране корисника одмах након првог пријављивања.
- f) Корисник треба да има могућност промјене своје корисничке шифре без интервенције надлежног администратора.
- g) Трансфер корисничких шифара кроз комуникациону мрежу мора бити заштићен од могућности пресретања на мрежи и откривања.

Д. Доградња система заштите

Члан 22.

(1) Доградња система заштите вршиће се континуирано, у складу са резултатима процјене сигурности система, практичним искуствима нарушавања сигурности или покушаја за нарушавање сигурности система, развојем технологија, организационих и функционалних промјена, као и свих других аспеката који имају утицај на сигурност система.

(2) За сигурност система одговоран је систем администратор.

Е. Физичке мјере заштите

Члан 23.

За сваку организациону јединицу потребно је дефинисати:

- а) Правила приступа и кретања у просторијама за запослене и екстерни персонал ,
- б) Правила заштите машински читљивих података и штампаног материјала,
- с) Ограничења у копирању података,
- д) Правила транспорта података и докумената,
- е) Правила кориштења телефона, факсова, дигиталних камера итд.,
- ф) Остале мјере заштите (од пожара, поплава, губитка напајања електричном енергијом и слично).

КОНЗЕРВАТИВНЕ МЈЕРЕ ЗАШТИТЕ ПОДАТАКА V

Члан 24.

Конзервативне мјере се примјењују за случај да се догодио квар или напад на систем, и тада треба примијенити слиједеће кораке:

- а) Процијенити штету,
- б) Утврдити узрок и разлог проблема/хаварије,
- с) Отклонити квар/грешку и (или) посљедице хаварије/напада (примијенити правила политике и контроле мјере сигурности),
- д) Документовати догађај и примјењене поступке, извући закључке и по потреби ажурирати план сигурности и увести додатне мјере и поступке,
- е) Евентуално примијенити алтернативни план како би се обезбиједио континуитет активности система.

ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ VII

Члан 25.

Овај Правилник ступа на снагу осмог дана од дана објављивања у “Службеном гласнику Брчко дистрикта БиХ”.

Директор,
Мато Лучић, дипл.еџц