CRNA GORA
GLAVNI GRAD PODGORICA
CENTAR ZA INFORMACIONI SISTEM

PRAVILNIK
O
upotrebi i zaštiti resursa na računarsko-komunikacionoj mreži Glavnog grada Podgorica

Podgorica, jul 2015. godine

IDENTIFIKATOR DOKUMENTA

Organizacija:	GLAVNI GRAD PODGORICA
Organizaciona jedinica:	CENTAR ZA INFORMACIONI SISTEM
Naziv dokumenta:	**Pravilnik o upotrebi i zaštiti resursa na računarsko-komunikacionoj mreži Glavnog grada Podgorica**
Osnov donošenja:	Izvještaj Službe za unutrašnju reviziju
Period na koji se donosi:	Trajno – do nove izmjene
Jezik:	Službeni jezik u CG
Odgovoran:	Direktor Zoran Glomazić, dipl. ing. el.
Kome se podnosi:	Gradonačelnik, Zamjenici gradonačelnika, Glavni administrator
Datum nastanka:	Jul 2015.
Broj verzije:	Ver. 1.3
Status:	Konačno

Pravilnik
o upotrebi i zaštiti računarsko-komunikacionih resursa na mreži Glavnog grada Podgorica

Predmet pravilnika

Član 1

Ovim Pravilnikom se propisuje način upotrebe i zaštite resursa na računarsko-komunikacionoj mreži Glavnog grada Podgorica, kojom upravlja Centar za informacioni sistem (u daljem tekstu: CIS), u skladu sa Odlukom o organizaciji Glavnog grada, a u cilju obezbjeđivanja njenog logičkog i fizičkog integriteta.

CIS vrši poslove administracije i održavanja računarskih resursa, periferija, softvera, mreže i mrežne infrastrukture u svojoj nadležnosti, kao i utvrđivanje tehničkih i drugih pravila upotrebe računarsko-komunikacionih resursa na mreži.

Ovaj Pravilnik se primjenjuje na sve organizacione jedinice Glavnog grada, gradske opštine, javne ustanove i preduzeća čiji je osnivač Glavni grad (u daljem tekstu: organizacione jedinice), ako ostvaruju pristup mreži.

Značenje pojedinih izraza

Član 2

Pojedini izrazi upotrijebljeni u ovom Pravilniku imaju sljedeće značenje:

1. ***Računarsko-komunikacioni resursi*** na mreži obuhvataju:
   - Računare i računarsku opremu (radne stanice, prenosni računari, serveri, storidži, štampači, skeneri, UPS, mrežno komunikaciona oprema...);
   - Servise na mreži koji uključuju: sistem upravljanja korisničkim nalozima i centralizovanu administraciju mrežnih resursa, elektronsku poštu na domenu mreže i van mreže, upotrebu Interneta, antivirusnu zaštitu;
2. ***Korisnik*** je lice zaposleno u organizacionoj jedinici iz stava 3 član 1 koje koristi računarsko-komunikacione resurse na mreži;
3. ***Korisnički nalog*** je instrument koji omogućava autorizovani (legalni) pristup infrastrukturnim servisima i resursima mreže i sadrži korisničko ime i lozinku pomoću kojih se korisnik prijavljuje na mrežu i identifikuje u sistemu;
4. ***Korisničko ime*** je jedinstveno javno ime korisnika kojim se on predstavlja sistemu i drugim korisnicima i kreira se na osnovu pravila utvrđenih u CIS-u;
5. ***Lozinka*** je tajna šifra korisnika, koja se u kombinaciji sa korisničkim imenom koristi za pristup sistemu;
6. ***Administrator sistema*** je ovlašćeno tehničko lice koje vrši administraciju korisničkih naloga na mreži i administraciju sistema;
7. ***Elektronska pošta*** je servis koji omogućava slanje i primanje poruka elektronskim putem kroz internet;

8. ***Mail client*** je program za korišćenje elektronske pošte;
9. ***Internet*** je javno dostupna mreža podataka koja povezuje računare i računarske mreže korišćenjem različitih mrežnih protokola;
10. ***Antivirusna zaštita*** obuhvata uređaje i programe napravljene da zaštite računare na taj način što pokušavaju pronaći, spriječiti i ukloniti računarske viruse.

Zaštita računara i računarske opreme

Član 3

Računarsko- komunikacioni resursi: serveri, stoni i prenosni računari i mobilni uređaji, periferijska oprema, kao i hardver računarke mreže su vlasništvo Glavnog grada i namijenjeni su korišćenju u poslovne svrhe od strane lica zaposlenih u organizacionim jedinicama.

Nijedan zaposleni ne smije hardver koji privatno posjeduje koristiti ili instalirati na računarima i/ili u računarskoj mreži Glavnog grada. Takav hardver predstavlja prijetnju integritetu i sigurnosti računara i računarske mreže.

Kada postanu svjesni upotrebe privatnog hardvera u svojoj organizaciji, zaposleni su u obavezi da upozore svog rukovodioca i zaposlene u Centru za informacioni sistem.

Iznošenjem prenosivog računara izvan prostorija Glavnog grada zaposleni preuzima punu odgovornost za njegovo čuvanje, hardver, softver i podatke.

Član 4

Obaveza Glavnog grada je da upravlja svojim softverskim resursima i korišćenjem softvera, tako da se za sve zaposlene koji koriste računar u procesu rada:

- Pribavi, reprodukuje, održava, dijeli, prenosi i koristi računarski softver u skladu sa zakonima Crne Gore i međunarodnim standardima;
- Održava samo legalan softver na računarima i računarskoj mreži Glavnog grada.

Zaposleni ne smiju koristiti softver za koji Glavni grad nema odgovarajuću licencu.

Kada postanu svjesni upotrebe ili distribucije neautorizovanog (nelicenciranog) softvera u svojoj organizaciji, zaposleni su u obavezi da upozore svog rukovodioca i CIS.

Zaposleni ne smiju pozajmiti ili dati drugom licu softver koji je licenciran za Glavni grad.

Član 5

Nijedan zaposleni ne smije softver koji privatno posjeduje koristiti ili distribuirati na računarima i/ili u računarskoj mreži Glavnog grada. Takav softver predstavlja prijetnju integritetu i sigurnosti računara i računarske mreže Glavnog grada.

Na Internetu je dostupan veliki izbor softvera. Neki od tih softvera, poznati kao "freeware" ili "shareware", su dostupni besplatno za ograničene potrebe i mogu se instalirati na računar korisnika uz prethodno odobrenje CIS-a.

Ostali softveri dostupni na Internetu ili drugim elektronskim izvorima, traže kupovinu licence uz određenu finansijsku nadoknadu. Nijedan zaposleni ne smije instalirati takav softver na svoj računar bez prethodnog odobrenja CIS-a.

Član 6

Zaposleni može biti pozvan na odgovornost zbog postojanja bilo kog softvera na računaru koji koristi, a za koji Glavni grad nema odgovarajuću licencu. Posledice te neautorizovane upotrebe softvera idu od pismenog upozorenja, za manje nelegalne aktivnosti, do otkaza za slučaj namjerno ponovljenih nedozvoljenih radnji.

Član 7

Računari i računarska oprema koja je u nadležnosti organizacionih jedinica Glavnog grada, mora biti obezbijeđena u skladu sa usvojenom Uredbom o mjerama informacione bezbjednosti.

Korisnik je dužan da obezbijedi fizičku sigurnost računara, računarske opreme i okruženja za opremu koju koristi, kako ne bi došlo do mogućnosti zloupotrebe podataka na istom, (a u najmanjem obimu da):

- onemogući neovlašćen pristup računaru i računarskoj opremi;
- lozinkom zaštiti "screensaver" na svom računaru;
- obezbijedi uslove kako ne bi došlo do fizičkog oštećenja računara i računarske opreme (rizik od potencijalnih hemijskih uticaja, smetnji u električnom napajanju, uticaj temperature i vlage i sl.)
- prijavi saznanje o eventualnoj zloupotrebi pristupa računaru.

Konfiguracija opreme

Član 8

Svaki računar mora biti konfigurisan da posjeduje minimum uslova neophodnih za obavljanje redovnog posla, a to su:

- instaliran operativni sistem;
- da je učlanjen u domen;
- dodijeljeno odgovarajuće jedinstveno ime na mreži;
- instaliran korporativni antivirusni program;
- instaliran osnovni Office paket;
- instaliran web browser (neki od standardnih);
- instaliran softver za čitanje PDF fajlova ;
- instaliran program za arhiviranje fajlova ;
- konfigurisanu mrežnu karticu sa odgovarajućim parametrima za internet (DNS, proxy);

Softver instaliran na računarima i računarskoj opremi mora biti legalan.

Zabranjeno je samoinicijativno instaliranje softvera ili mijenjanje konfiguracije računara od strane korisnika.

Upotreba korisničkih naloga

Član 9

Pristup računarsko-komunikacionim resursima na mreži ostvaruje se preko korisničkog naloga na osnovu koga je korisnik jasno identifikovan na mreži.

Administraciju korisničkog naloga (otvaranje, suspenziju, ukidanje i ažuriranje) na domenu vrši administrator iz CIS-a.

Korisnik od administratora dobija podatke o korisničkom imenu i inicijalnoj lozinki, kojom aktivira korisnički nalog, nakon čega je dužan da promijeni inicijalnu lozinku.

CIS je dužan da obezbijedi zaštitu korisničkog naloga u skladu sa internim pravilima na nivou domena mreže.

Obaveze korisnika (nosioca naloga)

Član 10

Korisnik je odgovoran za sve aktivnosti na mreži nastale upotrebom njegovog korisničkog naloga.

Korisnik je u obavezi da:

- sva službena dokumenta u elektronskom obliku čuva na serverima u data centru, koristeći za to posebno namijenjen folder koji se nalazi na desktop-u računara;
- korisnički nalog koristi isključivo u poslovne svrhe, na način kako je to definisano radnim zadacima;
- prijavi sve uočene nepravilnosti ili zloupotrebe korisničkog naloga od strane drugog lica.

Ograničenja i odgovornost nosioca korisničkog naloga

Član 11

Korisniku je zabranjeno:

- da koristi tuđi korisnički nalog;
- da podatke o svom korisničkom nalogu saopštava drugom licu;
- da bez saglasnosti vlasnika informacija upotrebljava korisnički nalog u svrhu javnog izlaganja informacija, preko postojećih mrežnih servisa ili interneta;
- da koristi mrežne resurse na način koji nije odobren od strane starješine organa;
- bilo kakva zloupotreba korisničkog naloga koja može ugroziti integritet podataka na mreži.

CIS nije odgovoran za eventualne štete koje bi nastale usljed (nepravilne) upotrebe korisničkog naloga, neadekvatnog korišćenja softvera ili hardvera, gubitka ili mijenjanja podataka ili njihovog izlaganja neovlašćenim licima, bez obzira da li je do štete došlo usljed greške korisnika ili nelegalne aktivnosti nepoznatog lica, omogućene nepažnjom korisnika.

Član 12

Svi podaci na svim računarima, računarskoj mreži i na svim informacionim sistemima koji se koriste u Glavnom gradu vlasništvo su Glavnog grada.

Glavni grad ima pravo da nadgleda korišćenje računara i sistema elektronske pošte u realnom vremenu kao i da provjerava zapise o ranijem korišćenju resursa (log fajlovi).

Glavni grad će izaći u susret obrazloženim zahtjevima regulatornih agencija i agencija za sprovođenje zakona za dostavljanje datoteka, poruka elektronske pošte, arhiva i log fajlova sa računara Glavnog grada.

Nijedan zaposleni ne smije da pristupi računaru drugog zaposlenog, porukama elektronske pošte i datotekama na računaru, bez prethodnog ovlašćenja.

Zaposleni su lično odgovorni za sve štete nastale nepridržavanjem bezbednosne politike Glavnog grada, autorskih prava i ugovora o licenciranju.

Preporuke za kreiranje lozinke

Član 13

Korisnik je dužan da izbjegava kreiranje "slabe" lozinke koja je:
- zasnovana na nečemu što se može lako pogoditi ili pronaći u ličnim podacima korisnika, kao što su imena, telefonski brojevi, datum rođenja i sl.;
- osjetljiva na napade koje koristi sistem rječnika (ne sastoje se od riječi iz rječnika);
- sastavljena od jednostavnih riječi koje su unazad napisane;
- kraća od 7 karaktera;
- jednostavna kombinacija brojeva i slova;
- sadrži samo niz jednakih znakova ili samo niz jednakih slova.

Korisnik je dužan da koristi "jaku" lozinku:
- minimalna dužina lozinke iznosi sedam karaktera;
- lozinka se sastoji od kombinacije velikih slova (najmanje jedno), malih slova, brojeva (najmanje jedan).

Zaštita lozinke

Član 14

Korisnik je dužan da vodi brigu o zaštiti lozinke.
Zaštita lozinke obezbjeđuje se tako što:
- se inicijalna lozinka mijenja prilikom prvog prijavljivanja na mrežu;
- lozinka koja se koristi na korisničkom nalogu bilo kojeg servisa na mreži ne smije biti ista sa lozinkom korisničkog naloga koji se koristi u privatne svrhe;
- zabranjeno je saopštavati svoju lozinku drugoj osobi;

- ako postoji bilo kakav nagovještaj da je ugrožen sistem ili lozinka, potrebno je promijeniti lozinku i prijaviti slučaj administratoru mreže;
- lozinke se mijenjaju u vremenskom intervalu od 42 dana, pri čemu nije moguća ponovna upotreba neke od posljednjih 20 lozinki;
- ne koristiti opciju „ZAPAMTI LOZINKU";
- ne pisati lozinke i pri tom ih nezaštićene držati na dohvat drugom licu;
- u posebnom slučaju, kada to odobri starješina organa, lozinka se može čuvati na bezbjednom mjestu (u koverti, sefu i sl.) kome pristup imaju samo ovlašćena lica.

Antivirus zaštita na mreži

Član 15

Antivirusna zaštita na mreži se sprovodi u cilju odbrane od virusa i druge vrste zlonamjernog koda koji u računarsku mrežu mogu dospjeti na više načina Internet konekcijom, e-mail-om, zaraženim prenosnim medijima (USB memorija, CD ...), instalacijom nelicenciranog softvera i sl.

CIS je dužan da sprovodi antivirusnu politiku na mreži i to na:

- centralnom nivou - upotrebom uređaja za filtriranje i usmjeravanje saobraćaja kao i upotrebom korporativnog antivirusnog softvera čime se spriječava "ulazak" malicioznog i neadekvatnog sadržaja sa Interneta;
- na korisničkom nivou - upotrebom antivirus programa na klijentskom računaru koji je sinhronizovan sa centralnim serverom;
- na nivou e-mail servera u cilju zaštite razmjene elektronske pošte.
- U cilju zaštite od virusa i malicioznih fajlova i podizanja nivoa bezbijednosti podataka u Glavnom gradu, zabranjeno je korisnicima korišćenje portabilnih uređaja tipa flesh meomorija, prenosnih hard diskova i sl. Bez izričite saglasnosti pretpostavljenog starješine i direktora CIS-a.

CIS je dužan da sa svoje strane obezbijedi korisniku sinhonizaciju klijentskog antivirus softvera sa centralnim antivirusnim serverom.

Obaveze korisnika u vezi sa antivirusnom zaštitom

Član 16

Korisnik je obavezan da:

- na svom računaru ima "aktiviran" antivirusni softver;
- periodično "skenira" fajlove;
- prijavi neadekvatno funkcionisanje antivirusnog softvera ili sumnju na postajanje virusa na računaru.

Korisnik ne smije svojevoljno mijenjati konfiguraciju i parametre antivirusnog softvera.

Upotreba Interneta

Član 17

Internet link je u vlasništvu Glavnog grada, ograničenog je kapaciteta i namijenjen za korišćenje u poslovne svrhe.

Pristup Internetu je, u okviru obavljanja poslovnih aktivnosti, dozvoljen ukoliko to nije drugačije odlučeno od strane starješine organa ili CIS-a.

Nedozvoljena upotreba Interneta

Član 18

Neprikladno, neprihvatljivo korišćenje Interneta je ono koje uzrokuje probleme u radu servisa koji su neophodni za obavljanje poslova u organizacionim jedinicama Grada.

Neprihvatljiva, odnosno nedozvoljena upotreba Interneta podrazumijeva:

- instaliranje, distribuciju, oglašavanje, prenos ili na drugi način činjenje dostupnim „piratskih" ili drugih softverskih proizvoda koji nisu licencirani na odgovarajući način;
- narušavanje sigurnosti mreže ili na drugi način remećenje poslovne Internet komunikacije;
- namjerno širenje destruktivnih i opstruktivnih programa na Internetu (Internet virusi, Internet trojanski konji, Internet crvi i druga vrsta malicioznih softvera);
- nedozvoljeno korišćenje društvenih mreža i drugih internet sadržaja koje je ograničio nadležni organ ili starješina organa;
- download (skidanje) podataka velike "težine" koje prouzrokuje "zagušenje" na mreži;
- download (skidanje) materijala zaštićenih autorskim pravima;
- korišćenje linkova koje nije povezano sa poslom (gledanje filmova, audio i videostreaming i sl.);
- neautorizovani pristup sadržaju, promena sadržaja, brisanje ili bilo kakva prerada sadržaja preko interneta.

Korisnicima koji neprikladnim korišćenjem Interneta uzrokuju zagušenje, prekid u radu ili dovedu u pitanje bezbjednost mreže može se oduzeti pravo pristupa Internetu.

Korišćenje računarskih resursa Glavnog grada i Interneta u svrhu pristupa, prenosa, arhiviranja ili distribucije zabavnog, rasističkog, seksističkog, prijetećeg ili drugog neprikladnog materijala je strogo zabranjeno. Materijal se definiše kao vizuelni, tekstualni ili audio fajl, stranica ili drugi elektronski entitet.

CIS zadržava pravo da reguliše Internet saobraćaj u mreži, odnosno da onemogući ili ograniči pristup pojedinim sajtovima.

Prava i obaveze korisnika

Član 19

Korisnik je dužan da koristi računarsko-komunikacione resurse savjesno, odgovorno, isključivo u poslovne svrhe kako ne bi ugrozio bezbjednost funkcionisanja mreže.

Korisnik je dužan da se pridržava odredbi ovog Pravilnika.

Korisnik je dužan da obavijesti CIS ili starješinu organizacione jedinice, ukoliko ima informacije o zloupotrebi računarsko-komunikacionih resursa od strane drugog lica.

Dostupnost resursa

Član 20

CIS omogućava korisniku dostupnost mrežnih servisa 24 časa, sedam dana u nedelji (24/7) a u skladu sa poslovnim pravilima i radnim zadacima korisnika, osim u slučaju nepredviđenih tehničkih problema.

Kaznene odredbe

Član 21

U slučaju nepoštovanja odredbi ovog Pravilnika, CIS zadržava pravo uskraćivanja pristupa računarsko-komunikacionim resursima korisniku i svih prava koja iz toga proističu.

Završne odredbe

Član 22

Pravilnik stupa na snagu danom potpisivanja.

Broj: 12-D1-032-2288/2015
Podgorica,03. jul 2015. godine

DIREKTOR CIS-A
Zoran Glomazić, dipl. ing. el.