Na osnovu člana 38 Zakona o državnoj upravi ("Službeni list RCG", broj 38/03 i "Službeni list CG", br. 22/08 i 42/11), Ministarstvo za informaciono društvo i telekomunikacije donijelo je

Pravilnik

o upotrebi računarsko-komunikacionih resursa na mreži državnih organa

Predmet

Član 1

Ovim pravilnikom propisuje se način upotrebe računarsko-komunikacionih resursa na mreži organa državne uprave (u daljem tekstu: mreža), kojom upravlja organ državne uprave nadležan za poslove informacionog društva (u daljem tekstu: Ministarstvo).

Primjena

Član 2

Ovaj pravilnik primjenjuje se na sve zaposlene u državnim organima koji ostvaruju pristup mreži (u daljem tekstu: korisnici).

Značenje izraza

Član 3

Izrazi upotrijebljeni u ovom pravilniku imaju sljedeća značenja:

1) **računarsko-komunikacioni resursi** su računari, računarska oprema, mrežno komunikaciona oprema i servisi na mreži;
2) ***korisnički nalog*** je instrument koji omogućava pristup infrastrukturnim servisima i resursima mreže i sadrži korisničko ime i lozinku pomoću kojih se korisnik prijavljuje na mrežu;
3) ***korisničko ime*** je jedinstveno ime korisnika kojim se predstavlja drugim korisnicima ;
4) ***lozinka*** je tajna šifra korisnika;
5) ***administrator*** je ovlašćeno tehničko lice u Ministarstvu koje vrši pružanje usluga u vezi korisničkih naloga na mreži;
6) ***elektronska pošta*** je servis koji omogućava slanje i primanje poruka elektronskim putem i predstavlja način službene komunikacije;
7) ***internet*** je javno dostupna mreža podataka koja povezuje računare i računarske mreže korišćenjem različitih mrežnih protokola;
8) ***antivirusna zaštita*** je skup uređaja i programa napravljenih radi zaštite računara na način da mogu pronaći, spriječiti i ukloniti računarske viruse.
9) ***mail client*** je program za korišćenje elektronske pošte.

Računarsko-komunikacioni resursi

Član 4

Računarsko-komunikacioni resursi na mreži obuhvataju:

- računare i računarsku opremu (radne stanice, prenosni računari, serveri, štampači, skeneri, mrežno komunikaciona oprema i td.);
- 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.

Zaštita računara i računarske opreme

Član 5

Korisnik obezbjeđuje zaštitu računara i računarske opreme, da ne bi došlo do zloupotrebe njihovih podataka, na način da:

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

Zaštita računara i računarske opreme vrši se u skladu sa propisom kojim se uređuju mjere informacione bezbjednosti.

Konfiguracija opreme

Član 6

Računar mora biti konfigurisan na način da ispunjava minimalne uslove neophodne za njegovo funkcionisanje, i to, da je:

1) učlanjen u domen;
2) instaliran operativni sistem;
3) dodijeljeno odgovarajuće korisničko ime na mreži;
4) instaliran korporativni antivirusni program;
5) instaliran osnovni Office paket;

6) instaliran Web Browser;
7) instaliran softver za čitanje PDF fajlova ;
8) instaliran program za arhiviranje fajlova ;
9) konfigurisana mrežna kartica sa odgovarajućim parametrima za internet (DNS, proxy).

Softveri koji se instaliraju na računarima i računarskoj opremi moraju biti licencirani.

Samoinicijativno instaliranje softvera ili mijenjanje konfiguracije računara korisnik ne može vršiti.

Upotreba korisničkih naloga

Član 7

Pristup mreži ostvaruje se preko korisničkog naloga na osnovu kojeg je korisnik identifikovan na mreži.

Pružanje usluga u vezi korisničkog naloga (otvaranje, suspenzija, ukidanje i ažuriranje) na domenu vrši administrator.

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

Korisnik je odgovoran za sve aktivnosti na mreži koje se vrše upotrebom njegovog korisničkog naloga.

Korisnik upotrebljava korisnički nalog isključivo u poslovne svrhe, na način utvrđen radnim zadacima i prijavljuje sve uočene nepravilnosti ili zloupotrebe korisničkog naloga od strane drugog lica.

Ograničenja upotrebe korisničkog naloga

Član 8

Korisnik ne može da:

- koristi tuđi korisnički nalog;
- podatke o svom korisničkom nalogu saopštava drugom licu;
- bez saglasnosti lica koje posjeduje određene informacije upotrebljava korisnički nalog radi javnog isticanja informacija, preko postojećih mrežnih servisa;
- koristi mrežne resurse na način koji nije odobren od strane starješine organa;
- vrši zloupotrebu korisničkog naloga na način kojim bi se ugrozila tajnost podataka na mreži.

Preporuke za kreiranje lozinke

Član 9

Korisnik treba da izbjegava korišćenje “slabe” lozinke koja je:

- kreirana na način da se može lako pogoditi ili pronaći u ličnim podacima korisnika, (ime, telefonski broj, 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 sedam karaktera;
- jednostavna kombinacija brojeva i slova;
- sadrži samo niz jednakih znakova ili samo niz jednakih slova.

Korisnik treba da koristi “jaku” lozinku, na način da:

- minimalna dužina lozinke iznosi sedam karaktera;
- se lozinka sastoji od kombinacije velikih slova (najmanje jedno), malih slova, brojeva i najmanje dva specijalna karaktera (!,#,$,%,&,?,@,{,}...).

Zaštita lozinke

Član 10

Zaštita lozinke obezbjeđuje se na način da:

1) se inicijalna lozinka mijenja prilikom prvog prijavljivanja na mrežu;
2) 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;
3) se lozinka ne saopštava drugom licu;
4) ako postoji sumnja da je ugrožen sistem ili lozinka, se promijeni lozinka i slučaj prijavi administratoru mreže;
5) se lozinke mijenjaju u roku od 42 dana , i da se ne vrši ponavljanje jedne od posljednjih 20 lozinki;
6) ne treba koristiti opciju „ZAPAMTI LOZINKU“;
7) se lozinke ne pišu na mjestu dostupnom drugim licima;
8) izuzetno, uz pretnodno odobrenje starješine organa, lozinka se može čuvati na bezbjednom mjestu (u koverti, sefu i sl.), kojem pristup imaju samo ovlašćena lica,

Antivirus zaštita na mreži

Član 11

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

Antivirusna zaštita na mreži obezbjeđuje se na:

- centralnom nivou - upotrebom uređaja za filtriranje i usmjeravanje saobraćaja kao i upotrebom korporativnog antivirusnog softvera čime se spriječava "ulazak" neadekvatnog sadržaja sa interneta;
- korisničkom nivou - upotrebom antivirus programa na računaru nosioca korisničkog naloga koji je sinhronizovan sa centralnim serverom i
- nivou e-mail servera radi zaštite razmjene elektronske pošte.

Antivirusna zaštita korisnika

Član 12

Korisnik treba 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.

Pristup internetu

Član 13

Pristup internetu je dozvoljen, radi obavljanja poslovnih aktivnosti, ako starješina državnog organa ili Ministarstva nije drugačije odlučio.

Nedozvoljena upotreba interneta

Član 14

Nedozvoljena upotreba interneta obuhvata:

- instaliranje, distribuciju, oglašavanje, prenos ili na drugi način činjenje dostupnim „piratskih“ ili drugih softverskih proizvoda koji nijesu licencirani na odgovarajući način;

- narušavanje sigurnosti mreže ili na drugi način onemogućavanje 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 ograničeno od Ministarstva ili na zahjtev starješine organa;
- preuzimanje (download) podataka velike "težine" koje prouzrokuje "zagušenje" na mreži;
- preuzimanje (download) materijala zaštićenih autorskim pravima;
- korišćenje linkova koji nijesu u vezi sa poslom (gledanje filmova, audio i videostreaming i sl.);
- nedozvoljeni pristup sadržaju, promjena sadržaja, brisanje ili prerada sadržaja preko interneta.

Korisnicima koji neadekvatnim korišćenjem interneta uzrokuju zagušenje, prekid u radu ili narušavaju bezbjednost mreže može se oduzeti pravo pristupa.

Upotreba elektronske pošte

Član 15

Servis elektronske pošte dostupan je putem posebnih softvera (mail client) koji su instalirani i konfigurisani na računarima korisnika ili putem internet adrese (https://mail.gov.me/owa/).

Servis elektronske pošte povezan je sa sistemom za upravljanje korisničkim nalozima na način da se pristup e-mail nalogu omogući upotrebom domenskog naloga.

Servis elektronske pošte obezbjeđuje primanje/slanje elektronskih poruka, dijeljenje adresara, kalendar, antispam zaštitu i arhiviranje elektronske pošte.

Radi efikasnije upotrebe elektronske pošte korisnik:

- redovno arhivira elektronske poruke zbog ograničene veličine poštanskog sandučeta (mailbox-a);
- redovno briše nepotrebnu poštu;
- obezbjeđuje da sadržaj poruka bude u skladu sa preporukama poslovne korespodenicije (formalno obraćanje, prikladno i jasno izražavanje, korišćenje našeg alfabeta).

Ograničenja prilikom upotrebe elektronske pošte

Član 16

Nedozvoljena upotreba elektronske pošte obuhvata:

- uznemiravanje korisnika elektronske pošte, načinom izražavanja i količinom poruka;
- kreiranje ili prosljeđivanje „lančanih pisama“ ili drugih „piramidalnih šema“, kao i slanje istovjetnih neželjenih poruka na veliki broj e-mail adresa („spam“);
- korišćenje službenog mail-a u privatne svrhe, reklamiranje proizvoda i uznemiravanje drugih zaposlenih.

Korisniku koji zloupotrebljava pristup mreži Ministarstvo će ukinuti pravo pristupa mreži o čemu obavještava starješinu organa i ovlašćeno lice korisnika.

Upotreba resursa

Član 17

Računarsko-komunikacione resurse korisnik upotrebljava savjesno i odgovorno, isključivo u poslovne svrhe da ne bi ugrozio bezbjednost funkcionisanja mreže.

Korisnik treba da obavijesti Ministarstvo ili starješinu organa, ako ima informacije o zloupotrebi računarsko-komunikacionih resursa od strane drugog lica.

Dostupnost resursa

Član 18

Mrežni servisi dostupni su 24 časa, sedam dana u nedelji, osim u slučaju nepredviđenih tehničkih problema.

Stupanje na snagu

Član 19

Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja u „Službenom listu Crne Gore“.

Broj: 051-01-2004/1-13

Podgorica, 05.07.2013. godine

MINISTAR

Prof.dr Vujica Lazović