Na osnovu člana 56a Zakona o naučnoistraživačkoj delatnosti (Sl. Gl. R.S. 110/05, 50/2006-ispr., 18/2010 i 112/2015), člana 38. Statuta Instituta za nuklearne nauke „Vinča" i predloga i preporuke Upravnog tela AMRES-a datih u Pravilniku o korišćenju Akademske mreže Srbije i Pravilniku zaštite i korišćenja lozinki AMRES-a, direktor Instituta za nuklearne nauke „Vinča", ul. Mike Petrovića – Alasa br. 12-14, Beograd - Vinča dana 13.05.2016. godine doneo je

PRAVILNIK
O UPOTREBI RAČUNARSKO-KOMUNIKACIONIH RESURSA NA MREŽI VincaNet

Predmet

Član 1.

Ovim pravilnikom propisuje se:

1) dozvoljeno i nedozvoljeno korišćenju resursa Instituta „Vinča" i drugih resursa dostupnih preko mreže AMRES korisnika,
2) obaveze korisnika, npr. čuvanje lozinki, zabrana prenosa korisničkih prava na druga lica itd.,
3) prava i obaveze Instituta „Vinča", a prema raspoloživim tehničkim mogućnostima,
4) prekršaji pravilnika, kao i sankcija za te prekršaje u smislu utvrđivanja aktivnosti koje se preduzimaju u slučaju značajnijih, učestalih ili zlonamernih prekršaja, napada na resurse ili u drugim slučajevima opasnim po funkcionalnost servisa.

Primena

Član 2.

Ovaj pravilnik primjenjuje se na sve zaposlene u Institutu za nuklearne nauke „Vinča" koji ostvaruju pristup računarskoj mreži VincaNet (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 Institutu koje vrši pružanje usluga u vezi korisničkih naloga na mreži;
6) **elektronska pošta** (e-mail) 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, sprečiti 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 itd.);
- ✓ 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.

Računarsko-komunikacione resurse korisnik upotrebljava savesno i odgovorno, isključivo u poslovne svrhe.

Korisnik je dužan da obavesti administratora ili direktora Instituta, ako ima informacije o zloupotrebi računarsko-komunikacionih resursa od strane drugog lica.

Zaštita računara i računarske opreme

Član 5.

Korisnici 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; obezbedi 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.

Konfiguracija opreme

Član 6.

Računar mora biti konfigurisan na način da ispunjava minimalne uslove neophodne za njegovo funkcionisanje, i to, da mu je:
1) dodeljena IP adresa od strane administratora;
2) instaliran operativni sistem;
3) dodeljeno odgovarajuće korisničko ime na mreži, koje može odobriti samo administrator;

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

Korisnik ne sme vršiti, samoinicijativno dodeljivanje i menjanje IP adrese.

Upotreba korisničkih naloga

Član 7.

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

Korisnički nalog je službeni i vlasništvo je Instituta "Vinča".

Korisnički nalog se dodeljuje zaposlenima Instituta "Vinča". U izuzetnim slučajevima može se dodeliti drugim licima, po nalogu direktora Instituta, u svrhu omogućavanja bolje komunikacije učesnika u realizaciji naučnoistraživačkih projekata.

Pružanje usluga u vezi korisničkog naloga (otvaranje, suspenzija, ukidanje i ažuriranje) na domenu vrši administrator, po nalogu direktora organizacione jedinice ili direktora Instituta.

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

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

Nije dozvoljeno korišćenje korisničkog naloga u privatne svrhe radi reklamiranja proizvoda, direktne komercijalne aktivnosti u cilju ostvarivanja ličnog profita korisnika prodaje robe ili usluga, oglašavanja, uznemiravanje drugih zaposlenih, itd.

Svaki korisnik je dužan da prijavli sve uočene nepravilnosti ili zloupotrebe korisničkog naloga od strane drugog lica.

Administrator je u obavezi da garantuje privatnost komunikacije korisnika putem naloga.

Ograničenja upotrebe korisničkog naloga

Član 8.

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

Preporuke za kreiranje lozinke

Član 9.

Karakteristike nedovoljno sigurnih lozinki koje se ne smeju koristiti su:

- ✓ nedovoljan broj karaktera u sklopu lozinke,
- ✓ lozinka koja se može naći u rečniku srpskog ili stranog jezika
- ✓ lozinka koja se sastoji od porodičnih imena, imena kućnih ljubimaca, poznatih ličnosti ili filmskih junaka,
- ✓ lozinka koja se sastoji od kompjuterski termina, komandi, imena web sajtova ili proizvođača računarskog hardvera ili softvera
- ✓ lozinka koja se sastoji od datuma, telefonskih brojeva ili adrese
- ✓ lozinka koja se sastoji od sklopova slova ili brojeva kao što su aaabbb, qwerty, abcdefg, 123321 i slično

- ✓ bilo koji slučaj prethodno navedene lozinke napisan unazad ili kombinovan sa jednim brojem

Karakteristike dovoljno sigurnih lozinki koje se moraju koristiti su sledeće:

- ✓ sastoji se iz velikih i malih slova, brojeva i drugih alfanumeričkih karaktera,
- ✓ ima dužinu od minimalno 8 karaktera
- ✓ nije konkretna reč nijednog jezika ili slenga
- ✓ nije konstruisana na osnovu nekih ličnih informacija

Zaštita lozinke

Član 10.

Korisnici VincaNet-a u okviru AMRES servisa (npr. e-mail, web, dial-up...) su u obavezi da poštuju sledeća pravila:

1. lozinka koju AMRES krajnji korisnik koristi mora biti konstruisana prema preporukama za kreiranje lozinki navedenih u Pravilniku zaštite i korišćenja lozinki AMRES-a;
2. lozinka koju AMRES korisnik koristi na bilo kojem AMRES servisu ne sme biti ista sa lozinkom koju koristi na bilo kom drugom servisu privatne svrhe.
3. zabranjeno je deliti svoj korisnički nalog AMRES servisa i lozinku sa bilo kojom drugom osobom, kolegom ili korisnikom AMRES-a.
4. ne saopštavati nikome svoju lozinku. U slučaju da vam neko od nadređenih, administratora AMRES-a ili zaposlenih traži da mu saopštite vašu lozinku, pozvati se na ovaj dokument i uputiti ga da kontaktira AMRES servisni centar.
5. lozinke se ne smeju slati elektronskom poštom niti bilo kojim drugim vidom elektronske komunikacije.
6. menjati lozinku u vremenskom intervalu od godinu dana.

Preporuke bezbednosti lozinki koje nisu obavezne za krajnje korisnike VincaNet-a u okviru AMRES servisa, su:

1. ne koristiti opciju čuvanja lozinke u bilo kom računarskom programu (na primer, MS Outlook, Eudora, Internet Explorer, Mozilla Firefox i sl.);
2. ne čuvati lozinku na papiru niti na bilo kom elektronskom uređaju (na primer, prenosnom računaru, mobilnom telefonu, računaru unutar nekog fajla i sl.);
3. u slučaju sumnje da je lozinka otkrivena, prijaviti slučaj AMRES servisnom centru kroz Helpdesk službu i promeniti sve lozinke.

Ukoliko korisnik nije poštovao napred navedena pravila zaštite lozinke odgovoran je za štetu koja nastane "neovlascenim upadom" na njegov sistem.

Antivirus zaštita na mreži

Član 11.

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

Antivirusna zaštita na mreži obezbeđuje se na: centralnom nivou - upotrebom uređaja za filtriranje i usmeravanje saobraćaja kao i upotrebom korporativnog antivirusnog softvera čime se sprečava "ulazak" neadekvatnog sadržaja sa interneta i na korisničkom nivou - upotrebom antivirus programa na računaru nosioca korisničkog naloga.

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.

Pristup internetu

Član 13.

Pristup internetu je dozvoljen, radi obavljanja poslovnih aktivnosti, ako direktor Instituta nije drugačije odlučio.

Nedozvoljena upotreba interneta

Član 14.

Nedozvoljena upotreba interneta obuhvata:

1. instaliranje, distribuciju, oglašavanje, prenos ili na drugi način činjenje dostupnim „piratskih" ili drugih softverskih proizvoda koji nisu licencirani na odgovarajući način;
2. narušavanje sigurnosti mreže ili na drugi način onemogućavanje poslovne internet komunikacije;
3. namerno širenje destruktivnih i opstruktivnih programa na internetu (internet virusi, internet trojanski konji, internet crvi i druga vrsta malicioznih softvera);
4. nedozvoljeno korišćenje društvenih mreža i drugih internet sadržaja;
5. preuzimanje (download) podataka velike "težine" koje prouzrokuje "zagušenje" na mreži;
6. preuzimanje (download) materijala zaštićenih autorskim pravima;
7. korišćenje linkova koji nisu u vezi sa poslom (gledanje filmova, audio i videostreaminga i sl.);

Korisnicima koji neadekvatnim korišćenjem interneta uzrokuju zagušenje, prekid u radu ili narušavaju bezbednost 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://www.vin.bg.ac.rs/).

Servis elektronske pošte obezbeđuje primanje/slanje elektronskih poruka, deljenje 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; obezbeđuje 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:

1. uznemiravanje korisnika elektronske pošte, načinom izražavanja i količinom poruka;
2. kreiranje ili prosleđivanje „lančanih pisama" ili drugih „piramidalnih šema", uznemiravanje, dosađivanje, ometanje ili onemogućavanje rada drugih korisnika, bez ustanovljenog opravdanog razloga, čak i u maloj meri (npr. spam e-mail, nastavak slanja e-mail-a osobi koja zatraži da joj se e-mail više ne šalje itd.).
3. Širenje nacionalne, verske, rasne ili polne diskriminacije, mržnje i netrpeljivosti, ili druge aktivnosti koje vređaju, kleveću ili uznemiravaju pojedince ili čitave grupe ljudi, kao što su pretnje, povreda religioznih, etničkih, političkih ili drugih uverenja i sl.;
4. Stvaranje, objavljivanje ili prenos uvredljivih, klevetničkih, opscenih ili nepristojnih slika, podataka ili drugog materijala, ili bilo kojih podataka koji mogu biti protumačeni kao opscene ili nepristojne slike ili materijal, osim za odobrene, nadgledane i zakonom dozvoljene naučno-istraživačke i poslovne svrhe;
5. Neovlašćeno objavljivanje ili prenos ličnih podataka i povreda privatnosti pojedinaca ili podataka o organizacijama koji se mogu smatrati poverljivim, kao što su poslovne tajne, lozinke, brojevi platnih kartica, medicinski podaci, privatni telefonski brojevi itd.
6. Neopravdano korišćenje službenog mail-a u privatne svrhe u smislu reklamiranja proizvoda, direktne komercijalne aktivnosti u cilju ostvarivanja ličnog profita korisnika prodaje robe ili usluga, oglašavanja, uznemiravanje drugih zaposlenih.itd.
7. Neopravdano korišćenje službenog mail-a kojim se vrši bilo horizontalno bilo vertikalno zlostavljanje na radu (mobing).

Elektronske poruke sa više od 10 primalaca se smeju slati samo sa ovlašćenih naloga za takvo korišćenje. Ova ovlašćenja izdaje direktor instituta.

Član 17.

Korisniku koji zloupotrebljava pristup mreži administrator će samoinicijativno ili po nalogu direktora organizacione jedinice odnosno direktora Instituta ukinuti pravo pristupa mreži.

Ukoliko administrator korisniku koji zloupotrebljava pristup mreže samoinicijativno ukine pravo pristupa mreži o tome obaveštava direktora Instituta "Vinča".

Zaposlenom koji je nedozvoljeno upotrebljavao internet ili elektronsku poštu na način opisan u članovima 14. i 16. ovog Pravilnika, kao i samoinicijativno dodeljivao i menjao IP adresu, direktor Instituta (Poslodavac) može da kazni:

1. Opomenom sa najavom otkaza, u kojoj se navodi da će poslodavac zaposlenom otkazati ugovor o radu bez ponovnog upozorenja, ako u narednom roku od šest meseci učini istu povredu,

2. privremeno udalji sa rada bez naknade zarade, u trajanju od jednog do 15 radnih dana,
3. novčanom kaznom u visini do 20% osnovne zarade zaposlenog za mesec u kome je novčana kazna izrečena, u trajanju do tri meseca, koja se izvršava obustavom od zarade, na osnovu rešenja poslodavca o izrečenoj meri;

Zaposlenom koji je nedozvoljeno upotrebljavao internet ili elektronsku poštu na način opisan u članovim 14. i 16. ovog Pravilnika, kao i samoinicijativno dodeljivao i menjao IP adresu, čime je pričinio štetu Institutu u vrednosti većoj od 1.000.000,00 RSD, direktor Instituta (Poslodavac) može u roku od 8 dana od dana dostavljanja upozorenja pred otkaz da otkaže ugovor o radu.

Poslodavac ima pravo na naknadu štete koju je Institutu pričinio zaposleni koji je nedozvoljeno upotrebljavao internet ili elektronsku poštu na način opisan u članovim 14. i 16. ovog Pravilnika, kao i samoinicijativno dodeljivao i menjao IP adresu u visini koju utvrđuje posebna komisija koju obrazuje direktor.

Ako zaposleni ne naknadi štetu prema odluci komisije, poslodavac će pokrenuti postupak za naknadu štete pred nadležnim sudom.

Poslodavac ima pravo da vrši uvid u elektronsku poštu sa službene e-mail adrese u okviru službene korespondencije.

Dostupnost resursa

Član 18.

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

Prelazne i završne odredbe

Član 19.

Na sve što nije regulisano ovim Pravilnikom, primenjivaće se odredbe Pravilnika o korišćenju Akademske mreže Srbije i Pravilnika zaštite i korišćenja lozinki.

Član 20.

Pravilnik o upotrebi računarsko-komunikacionih resursa na mreži VincaNet-a, donosi direktor Instituta.

Izmene i dopune ovog Pravilnika vrše se na isti način i po postupku po kome je i donet.

Član 21.

Ovaj Pravilnik stupa na snagu osmog dana od dana njegovog donošenja i objavljivanja na oglasnoj tabli i Web sajtu Instituta .

ИНСТИТУТ ЗА НУКЛЕАРНЕ НАУКЕ "ВИНЧА" БЕОГРАД

DIREKTOR INSTITUTA "VINČA"

dr Borislav Grubor