KLASA: 602-04/15-01/02
URBROJ: 2170-57-01-15-71

U Rijeci, 24. ožujka 2015. godine

Na temelju članka 59. stavka 2. alineje 11. Zakona o znanstvenoj djelatnosti i visokom obrazovanju („Narodne novine" broj: 123/03, 198/03, 105/04, 174/04, 2/07 - OUSRH, 46/07, 45/09, 63/11, 94/13, 139/13 i **101/14 - O i RUSRH)** i članka 59. stavka 1. alineje 3. Statuta Sveučilišta u Rijeci (pročišćeni tekst od 10. prosinca 2008. godine i Odluka o izmjenama i dopunama Statuta iz 16. ožujka 2010. godine, 19. studenog 2013. godine i 22. srpnja 2014. godine), Senat Sveučilišta u Rijeci je na svojoj 75. sjednici održanoj dana 24. veljače 2015. godine donio sljedeći

# PRAVILNIK O SIGURNOSTI INFORMACIJSKIH SUSTAVA SVEUČILIŠTA U RIJECI

## Uvodne odredbe

### Članak 1.

Ovim se Pravilnikom uređuje upravljanje sigurnošću informacijskih sustava na Sveučilištu u Rijeci (dalje: Sveučilište), definiraju prihvatljivi načini ponašanja i jasna raspodjela uloga i odgovornosti svih čimbenika informacijskog sustava.
Novi zaposlenici dužni su se upoznati s njegovim odredbama prilikom zapošljavanja, a studenti prilikom otvaranja korisničkih računa.
Pravila rada i ponašanja koja su definirana sigurnosnom politikom odnose se na:

- svu računalnu opremu koja se koristi u prostorima Fakulteta,
- administratore informacijskih sustava,
- korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti,
- vanjske tvrtke koje po ugovoru rade na održavanju opreme ili softvera.

## Organizacija upravljanja sigurnošću

### Članak 2.

Osobe koji se u radu koriste računalima i ostalim uređajima koji se priključuju na IT infrastrukturu dijele se na davatelje i korisnike informatičkih usluga.
Davateljima informatičkih usluga smatraju se one osobe koje su zadužene za ispravnost i neprekidnost rada računala, mreže i informacijskog sustava. Samo davatelji smiju biti administratori računala koja se koriste na Sveučilištu. Iznimno, na opravdani zahtjev korisnika ili uprave može se imenovati administrator koji nije iz grupe davatelja informatičkih usluga. U tom slučaju ta osoba dužna je upoznati se s pravima i odredbama koje iz toge proizlaze te potpisati Izjavu o administriranju računala.
Korisnici informatičkih usluga su osobe koje se koriste računalima, komunikacijskim uređajima i svim ostalim uređajima koji se priključuju na IT infrastrukturu Sveučilišta, u svrhu rada, učenja, proizvodnje dokumenta, unosa podatke ili koriste informatičke usluge Sveučilišta, a pritom ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže.

Korisnici informatičkih usluga obvezuje se:

- pridržavati se pravila prihvatljivog korištenja, to jest ne koristiti računala za radnje koje nisu u skladu sa važećim zakonima Republike Hrvatske, etičkim i moralnim normama, Etičkim kodeksom Sveučilišta u Rijeci i sigurnosnom politikom Sveučilišta,
- izabrati kvalitetnu zaporku i povremeno je mijenjati,

- čuvati autentifikacijske atribute za pristup računalima i komunikacijskim uređajima na siguran način i ne otkrivati ih drugim osobama ni pod kojim uvjetima,
- prijaviti svaki sigurnosni incident,
- ukoliko korisnici u svom radu proizvode podatke i dokumente, odgovorni su za vjerodostojnost tih podataka, te za njihovo čuvanje kao i za izradu sigurnosnih kopija podataka,
- u slučaju oštećenja ili kvara računala i/ili komunikacijskog uređaja navedeno je potrebno prijaviti Sveučilišnom informatičkom centru u što je moguće kraćem roku,
- u slučaju krađe ili gubitka računala i/ili komunikacijskog uređaja navedeno je potrebno prijaviti ovlaštenim osobama na pojedinoj sastavnici ili odjelu u što kraćem mogućem roku,
- omogućiti neometani rad prilikom održavanja računala i/ili komunikacijskih uređaja davateljima informatičkih usluga,
- prilikom uporabe Interneta ni pod kojim uvjetima se ne upuštati u aktivnosti koje su zakonski određene kao nelegalne,
- koristiti službenu elektroničku poštu Sveučilišta kao službeno sredstvo komunikacije,
- u slučaju dobivanja sumnjive elektroničke pošte postupati s razumnim oprezom te ne slijediti linkove i ne otvarati priloge koji se nalaze u elektroničkoj poruci, ukoliko je vjerodostojnost pošiljatelja upitna. O svim takvim porukama potrebno je odmah obavijestiti administratore IT sustava.

Korisnicima je zabranjeno:

- isključivanje i ometanje rada sustava za nadzor, upravljanje i zaštitu računala,
- neovlašteno kopiranje materijala na računalo koji je zaštićen pravom intelektualnog vlasništva, kopiranje zaštićenih fotografija, tekstova, filmova, glazbe, programa...,
- namjerno unošenje malicioznih programa u mrežne sustave i servere (npr.: virusi, crvi, trojanski konji...),
- odavanje svoje lozinke drugim osobama ili dopuštanje uporabe vlastitog korisničkog računa (user account) drugim osobama, neovisno o tome jesu li te osobe djelatnici Sveučilišta u Rijeci,
- namjerno uzrokovanje sigurnosnih incidenata koje uključuje, ali nije ograničeno na pristupanje podacima koji nisu namijenjeni korisniku ili uporabu korisničkog računa, za koji korisnik nema dozvolu za uporabu,
- neovlašteno konfiguriranje ili onemogućavanje/prekidanje rada mrežne i komunikacijske opreme,
- zaobilaženje autentifikacije i sigurnosnih mjera za pristup bilo kojem dijelu IT sustava,
- neovlašteno dodavanje/mijenjanje hardverske konfiguracije sustava ili dijela sustava (računala),
- neovlašteno mijenjanje sigurnosnih postavki računala i komunikacijskih uređaja,
- neovlašteno instaliranje programa,
- instaliranje i uporaba softvera na način da se krše prava intelektualnog vlasništva,
- korištenje neovlaštenih programa koji ne zahtijevaju instalaciju („portabilnih aplikacija") na računalu,
- slanje poruka koje sadrže podatke ili informacije protivno važećim sigurnosnim pravilima Sveučilišta,
- slanje poruka nedoličnog, lažnog i uvredljivog sadržaja te poruka s obmanjujućim sadržajem,
- slanje drugima reklamnih ili promotivnih materijale bez njihova pristanka ili traženja, uključujući slanje neželjenih elektroničkih poruka (spam e-mail),
- uznemirivanje putem elektroničke pošte u bilo kojem obliku kao npr. slanje velike količine neželjenih ili nezatraženih elektroničkih poruka na jedan korisnički račun,
- slanje ili prenošenje sadržaja koji nude usluge ili proizvode u obliku lančanih pisama,
- lažno predstavljanje ili davanje korisničkog imena i lozinke drugoj osobi, čime se omogućuje lažno predstavljanje, krivotvorenje zaglavlja poruke,

- objavljivanje sadržaja na Internetu bez suglasnosti vlasnika sadržaja te objavljivanje ili prenošenje netočnih, nepotpunih i uvredljivih podataka ili informacija,
- uporaba računala i komunikacijskih uređaja za neautorizirani pristup drugim računalima, mreži ili komunikacijskim uređajima preko Interneta ili ometanje drugih računala na Internetu.

**Članak 3.**

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima te treba osigurati njihovo čuvanje i pristup samo ovlaštenim osobama.
Ovlaštene osobe za čuvanje i pristup dokumentima u elektroničkom obliku imenuje čelnik Sveučilišta, tj. sastavnice sveučilišta.

**Članak 4.**

Davatelji informatičkih usluga dužni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti cjelokupnog IT sustava.
Imenovani administratori odgovorni su za instalaciju i konfiguraciju softvera na računalima u vlasništvu Sveučilišta. Ukoliko pojedini korisnici žele sami administrirati svoje osobno računalo, moraju potpisati izjavu o tome, nakon čega za njih vrijede ista pravila kao i za administriranje računala.

Računala se moraju konfigurirati na način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača operativnih sustava, listama pristupa, filtriranjem prometa i drugim sredstvima.
Posebnu pažnju administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa.
Davatelji informatičkih usluga ne smiju administrirati računala i mrežnu opremu koja je u vlasništvu privatnih i poslovnih korisnika.

**Članak 5.**

Administratori računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa. Zadaća je administratora i nadgledanje rada korisnika, kako bi se otkrile nedopuštene aktivnosti.

Administratori su dužni prijaviti incidente nadležnim službama i odgovornoj osobi na sastavnici, te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Nadležna služba za infrastrukturu za koju je odgovoran Sveučilišni informatički centar (SIC) je sam Sveučilišni informatički centar, dok je za infrastrukturu za koju nije odgovoran SIC nadležna informatička služba sastavnice. Ukoliko je incident ozbiljan i uključuje kršenje zakona Republike Hrvatske, prijavljuju se CARNet-ovom CERT-u.
Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla te moraju potpisati Izjavu o čuvanju povjerljivih informacija.

**Članak 6.**

Upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje mrežnih adresa, kreiranje virtualnih LAN-ova, te ostale poslove pri upravljanju mrežom na razini Kampusa Sveučilišta u Rijeci ili za infrastrukturu za koju je odgovoran Sveučilišni informatički centar (SIC) vrši Sveučilišni informatički centar.
Voditelj SIC-a može ovisno o raspoloživim kadrovskim resursima, imenovati odgovornu osobu za rad mreže.

Upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje mrežnih adresa, kreiranje virtualnih LAN-ova, te ostale poslove pri upravljanju mrežom na razini sastavnica Sveučilišta u Rijeci i za infrastrukturu za koju nije odgovoran Sveučilišni informatički centar (SIC) vrši informatička služba sastavnice.

**Članak 7.**

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. Korisnik koji ima potrebu za nekim programom, mora se obratiti koordinatoru za programsku podršku na sastavnici i zatražiti, uz obrazloženje, nabavu i instalaciju. Koordinator za programsku podršku na sastavnici poduzima daljnje radnje za nabavu softvera. Ako je sastavnica u sustavu SIC-a koordinator za programsku podršku na sastavnici o nabavi softvera obavijestit će sveučilišnog koordinatora za programsku podršku.

Sveučilišnog Koordinatora za programsku podršku imenuje rektor, a koordinatora za programsku podršku na sastavnici imenuje čelnik sastavnice.

**Članak 8.**

Povjerenstvo za sigurnost imenuje rektor, a sastavljeno je od prorektora za informatizaciju, CARNet koordinatora, voditelja SIC-a, predstavnika sastavnica koji nisu pod nadzorom SIC-a i predstavnika studenata.

Povjerenstvo prima izvještaje o sigurnosnoj situaciji i predlaže mjere za njeno poboljšanje, uključujući nabavu opreme, organizaciju obrazovanja korisnika i specijalista. Povjerenstvo daje odobrenje za provođenje istrage u slučaju incidenata.

Povjerenstvo podnosi izvještaj o stanju sigurnosti rektoru, te se zalaže za donošenje konkretnih mjera, nabavu potrebne opreme, ulaganje u obrazovanje specijalista, ali i običnih korisnika. U slučaju sigurnosnog incidenta prouzrokovanog od strane osoba koje nisu fakultetski korisnici, Povjerenstvo daje CARNet koordinatoru nalog za prijavu sigurnosnog incidenta CERT-u koji se nalazi u sastavu CARNet-a.

**Fizička sigurnost ključnih dijelova IT sustava**

**Članak 9.**

Prostor na ustanovi dijeli se na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposleni, te prostore u koje pristup imaju samo grupe zaposlenih, ovisno o vrsti posla koji obavljaju.

**Članak 10.**

Oprema koja obavlja ključne funkcije, neophodne za funkcioniranje informacijskog sustava ili sadržava povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama.

Ključna oprema treba biti zaštićena od problema s napajanjem električnom energijom, poplava, požara i sl. te treba poduzeti mjere da se oprema i informacije zaštite i da se osigura što brži popravak i ispravan rad. U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Za korisnike IT sustava pod upravljanjem SIC-a , voditelj centra za nadzor i upravljanje dužan je održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone. U pravilu su to samo zaposlenici koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje, obaviti servisiranje opreme.

Sastavnice čija IT infrastruktura nije pod upravljanjem SIC-a same određuju način nadzora.

**Članak 11.**

Za korisnike IT sustava pod upravljanjem SIC-a, u navedene prostorije pristup nije dozvoljen osobama koje nisu korisnici usluga, studentima, a dozvoljen je samo onim osobama koje je ovlastio rektor izravno ili putem Voditelja centra za nadzor i upravljanje.
Sastavnice čija IT infrastruktura nije pod upravljanjem SIC-a same određuju način nadzora.

**Članak 12.**

Povremeno se mora dopustiti pristup osobama iz vanjskih tvrtki ili ustanova, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.
Sveučilište, tj. njegove sastavnice, može u ugovore s vanjskim tvrtkama ugraditi odredbe kojima obavezuje poslovne partnere na poštivanje sigurnosnih pravila.
Vanjska tvrtka je dužna najaviti svaku svoju aktivnost ili intervenciju najmanje 24 sata prije aktivnosti.
Ugovorom će se regulirati pristup, čime se podrazumijeva pristup prostorijama, pristup opremi ili logički pristup povjerljivim informacijama. Treću stranu treba obavezati na čuvanje povjerljivih informacija s kojima dođu u dodir pri obavljanju posla.
Sveučilište može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, sigurnoj zoni ili osjetljivim informacijama potpiše Izjavu o čuvanju povjerljivih informacija.
Ako u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja.
Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je osiguran video nadzor.
Ukoliko se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podacima, Sveučilište će od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije Ustanove radi obavljanja posla.
U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Sveučilište.
Sveučilište zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ukoliko nisu na popisu ovlaštenih djelatnika.

**Sigurnost opreme**

**Članak 13.**

Sveučilište dijeli svu aktivnu i pasivnu opremu u grupe prema zadaćama:

- zona javnih servisa – oprema koja obavlja javne servise (DNS poslužitelj, web poslužitelj, poslužitelj elektroničke pošte itd.), i
- intranet je privatna mreža Sveučilišta, sačinjavaju je poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže,
- extranet je proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili povezuje izdvojene lokacije; u ovu grupu spadaju interni modemski ulazi (ako ih Fakultet ima), veze lokalnih baza podataka sa središnjim poslužiteljima (LDAP, ISVU, X-ice, baze knjižnice) i sl.

**Članak 14.**

Sveučilište je obavezno održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarskim brojevima itd.
Sveučilište je dužno osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi na Sveučilištu.
Za fizičku sigurnost opreme za infrastrukturu koja je u vlasništvu Sveučilišta u Rijeci odgovoran je rektor. On odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.
Za fizičku sigurnost opreme za infrastrukturu koja je u vlasništvu sastavnica Sveučilišta u Rijeci odgovorna je odgovorna osoba sastavnice. Oni odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.

Računalna oprema koja pripada Sveučilištu daje se korisnicima na raspolaganje radi obavljanja poslova vezanih uz redovno poslovanje Sveučilišta i nije ju dopušteno koristiti za obavljanje privatnih poslova korisnika.
Sveučilište zadržava pravo nadzora nad načinom korištenja računalne opreme. Privatna računala i računalnu opremu nije dopušteno priključivati na žičanu (Ethernet) računalnu mrežu Sveučilišta, osim uz odobrenje rektora, tj. odgovorna osoba sastavnice u slučaju da računalna mreža nije pod nadzorom SIC-a.
Računala i računalnu opremu nije dopušteno iznositi izvan prostora Sveučilišta bez uredno ovjerene Potvrde o korištenju opreme izvan Sveučilišta. Potvrdu izdaje čelnik sastavnice. Korisnici koji opremu koriste izvan prostora Sveučilišta odgovorni su za tu opremu kao i za sve posljedice koje proizlaze iz korištenja iste.

**Osiguranje neprekidnosti poslovanja**

**Članak 15.**

Kako bi se sačuvali podaci u slučaju nezgoda, kvarova na sklopovlju, požara ili ljudskih grešaka, neophodno je redovito izrađivati rezervne kopije svih podataka važnih za održavanje vitalnih funkcija informacijskog sustava i sklopovlja.
Prethodni stavak prvenstveno se odnosi na kopije sustava središnjih poslužitelja, knjižničnog poslužitelja, računovodstvenih podataka i podataka o konfiguraciji softvera neophodnog za funkcioniranje mreže.

**Članak 16.**

Za izradu rezervnih kopija podataka središnjih poslužitelja zaduženi su CARNet sistem inženjeri koji administriraju te poslužitelje. Za neprekidnost rada središnjeg poslužitelja odgovoran je administrator istog poslužitelja.
Za izradu rezervnih kopija podataka važnih za održavanje vitalnih mrežnih funkcija i računala važnih za podršku korisnicima, nadležna su djelatnici SIC-a koje imenuje voditelj.
Za izradu rezervnih kopija podataka važnih za održavanje vitalnih mrežnih funkcija i računala važnih za podršku korisnicima koji nisu pod nadzorom SIC-a, nadležna su djelatnici sastavnice Sveučilišta koje imenuje voditelj odgovorne službe.
Za izradu rezervnih kopija podataka knjižničnog poslužitelja zadužena je tvrtka s kojom Sveučilište tj. sastavnica ima ugovor o održavanju knjižnične programske podrške.
Za izradu rezervnih kopija računovodstvenih podataka zadužena je tvrtka s kojom Sveučilište tj. sastavnica ima ugovor o održavanju programske podrške.
U slučajevima u kojima Sveučilište ili sastavnica angažira vanjsku tvrtku za isporuku nestandardnog softvera, tvrtka koju odabere Sveučilište ili sastavnica dužna je osigurati sigurnosne kopije (backup) svih podataka vezanih uz pojedinu aplikaciju, kako na klijentskoj strani (korisnička računala) tako i na strani poslužitelja na kojem se pohranjuju podaci

**Članak 17.**

Sveučilište je dužno izraditi zaseban dokument u kojem se definiraju procedure za izradu rezervnih kopija, imenuju odgovorne osobe, određuje potrebna oprema, te prostor za čuvanje kopija.
Radi osiguranja neprekinutosti poslovanja, Sveučilište je dužno razraditi procedure za oporavak kritičnih sustava te ih čuvati u pismenom obliku, kako bi u slučaju zamjene izvršitelja novozaposleni djelatnici mogli brzo reagirati u slučaju nesreće. Dokumentaciju čuva voditelj SIC-a, tj. voditelj službe sastavnice koje nisu u sustavu SIC-a.
Osobe zadužene za izradu rezervnih kopija su dužne povremeno provjeravati upotrebljivost rezervnih kopija podataka, te izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na rezervnoj opremi, u laboratorijskim uvjetima.

**Korištenje računalne opreme Sveučilišta**

**Članak 18.**

Nedozvoljenim se smatra svako korištenje računala na način koji bi doveo do povrede važećih zakona, propisa ili etičkih normi, a mogao bi izazvati materijalnu ili nematerijalnu štetu za Sveučilište.
Lakšim oblicima nedozvoljenog korištenja računala i opreme smatra se:

- ograničena uporaba nelicenciranog softvera,
- skidanje (download) autorski zaštićenih datoteka bez plaćanja naknade ako su iste javno dostupne,
- skidanje (download) i(ili) distribucija sadržaja koji nije primjeren akademskoj zajednici (pornografija i sl.),
- slanje masovnih poruka, bile one komercijalne prirode ili ne, čime se nepotrebno troše mrežni resursi,
- samovoljna instalacija softvera,
- korištenje neprihvatljivih aplikacija i servisa zbog kojih se narušava sigurnost
- informacijskih sustava, nepotrebno troše mrežni resursi ili se nanosi bilo kakva materijalna i(ili) nematerijalna šteta Sveučilišta,
- korištenje računala Sveučilišta i ostalih informatičkih resursa Sveučilišta u svrhe koje nisu u skladu s Etičkim kodeksom Sveučilišta u Rijeci,
- korištenje mrežnih resursa Sveučilišta na način priključivanja vlastitih – privatnih računala na računalnu mrežu Sveučilišta.

Težim oblicima nedozvoljenog korištenja računala i opreme smatra se:

- preuzimanje tuđeg identiteta (korištenje opreme s tuđim korisničkim računom, slanje elektroničke pošte pod tuđim imenom, kupovanje preko interneta s tuđom kreditnom karticom itd.),
- provaljivanje na druga računala,
- traženje ranjivosti i sigurnosnih propusta; korisnik ne smije samoinicijativno skenirati računala, probijati zaporke ili na bilo koji način istraživati sigurnosne propuste na računalima, bilo da ona pripadaju Sveučilištu ili ne,
- napad uskraćivanjem resursa na druga računala,
- vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti,

**Članak 19.**

Djelatnici Sveučilišta u Rijeci, gostujući profesori i(ili) predavači na skupovima koji se održavaju u prostorijama Sveučilišta sami su dužni voditi računa o ispravnosti i sigurnosti osobnih računala koje koriste za predavanja, na skupovima, radionicama i slično.
Administratori IT sustava niti jednog trenutka ne preuzimaju odgovornost za eventualno nastalu štetu na osobnim računalima koja nisu konfigurirana u skladu s pravilnikom o korištenju računala i IT sustava.
Ukoliko Administratori IT sustava utvrde kako oprema nije u skladu sa sigurnosnim zahtjevima IT sustava Sveučilišta u Rijeci i može prouzročiti štetu (virusi, spyware, malware, piratski softver...) istu neće spajati na mrežnu i ostalu infrastrukturu IT sustava.

**Članak 20.**

Sveučilište zadržava pravo procjene prihvatljivog korištenja računalne opreme. Uprava Sveučilišta, tj. sastavnica, će sankcionirati neprihvatljive oblike korištenja računalne opreme na Sveučilištu sukladno težini neprihvatljivog korištenja, a na temelju procjene/mišljenja Povjerenstva za sigurnost.
Korisnici informatičkih resursa i opreme dužni su upozoriti upravu Sveučilišta, tj. sastavnica, na svaki oblik neprihvatljivog ponašanja korisnika, a prvenstveno su dužni svojim primjerom pozitivno utjecati na promicanje prihvatljivog ponašanja ostalih korisnika.

**Bežična mreža**

**Članak 21.**

Pristup bežičnoj mreži moguć je:

a) uz autentikaciju sukladno standardu eduroam (http://www.eduroam.hr/). U tom slučaju korisnik mora posjedovati odgovarajući elektronički identitet iz sustava AAI@EduHr ili globalnog sustava eduroam,
b) bežična mreža SSID: WLAN-INFO koristi se isključivo za pristup eduroam installeru (http://installer.eduroam.hr/). Eduroam installer omogućuje krajnjim korisnicima jednostavno i pouzdano konfiguriranje uređaja (računala, prijenosnika, pametnog telefona) za pristup mreži po eduroam standardu,
c) isključivo kao rješenje za privremene potrebe/posebne prigode (npr. u slučaju organizacije skupova ili događanja), sastavnice mogu zatražiti kreiranje posebnog načina pristupa bežičnoj mreži u slučaju da postojeći standardni načini pristupa (eduroam) ne odgovaraju potrebama ustanove u takvim prigodama. Obavezno je definirati period u kojemu će se koristiti tražena bežična mreža.

**Zaporke**

**Članak 22.**

Svi zaposlenici Sveučilišta, suradnici i studenti koji u svome radu koriste računala dužni su pridržavati se u nastavku navedenih pravila korištenja zaporki, dok su ih administratori dužni tehnički ugraditi u sve sustave koji to omogućavaju.

Minimalna dužina zaporke mora biti osam znakova. Za zaporku se ne smije koristiti riječi iz rječnika, niti imena bliskih osoba, ljubimaca, datume. U zaporci je obavezno korištenje malih i velikih slova u kombinaciji s brojevima. Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava. Korisnik je odgovoran za tajnost svoje zaporke, te mora naći način da je sakrije.

**Članak 23.**

Na računalima koja spadaju u zonu visokog rizika administratori su dužni konfigurirati sustav na taj način da se korisnički račun zaključa nakon pet neuspjelih pokušaja prijave.

Administratori su dužni konfigurirati autentikaciju tako da zaporke zastare nakon 180 dana, te onemogućiti korištenje zaporki koje su već potrošene, ako sustav to dozvoljava.

Prilikom provjere sustava sigurnosni tim može ispitati da li su korisničke zaporke u skladu s navedenim pravilima.

Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava. U slučaju ponovljenog ignoriranja ovih pravila Sveučilište može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogućnost ugrožavanja integriteta i sigurnosti sustava i podataka.

**Antivirusna zaštita i zaštita od spama**

**Članak 24.**

Zaštita od virusa je obavezna, a provode je davatelji informatičkih usluga nadležni za pojedini dio sustava, i to na:

- poslužiteljima elektroničke pošte – ovlašteni CARNet sistem inženjeri,
- na internim poslužiteljima Fakulteta – djelatnici SIC-a ili djelatnici sastavnice sveučilišta ili CARNet sistem inženjeri,
- svakom osobnom računalu korisnika – administratori računala.

Osobe koje provode zaštitu od virusa nisu dužne čuvati elektroničke poruke korisnika zaražene virusima.

**Članak 25.**

Osobe koje provode antivirusnu zaštitu dužne su instalirati antivirusne programe na sva korisnička računala i namjestiti ih tako da se izmjene u bazi virusa automatski propagiraju s središnje instalacije ili s vanjskog poslužitelja, bez aktivnog sudjelovanja korisnika.
Korisnici ne smiju samovoljno isključiti antivirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti antivirusni program, korisnici moraju zatražiti dozvolu od nadležnih davatelja informatičkih usluga ili administratora sustava.

**Članak 26.**

Administratori poslužitelja elektroničke pošte dužni su postaviti poslužitelje tako da prilikom primanja poruka konzultira baze podataka koje sadrže popise poslužitelja koji su otvoreni za odašiljanje (open relay), te baza s adresama poznatih „spamera". Pošta koja dolazi s tako pronađenih adresa neće se primati.
Osobe koje provode zaštitu od spama nisu dužne čuvati spam - poruke poslane korisnicima

**Nadzor nad informacijskim sustavima**

**Članak 27.**

Sveučilište zadržava pravo nadzora nad instaliranim softverom i podacima koji su pohranjeni na računalima, te nad načinom korištenja računala.
Nadzor se smije provoditi radi:

- osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa,
- provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident,
- provjere da li su informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.

Nadzor smiju obavljati samo osobe koje je Sveučilište, tj. sastavnica, za to ovlastilo. Pri provođenju nadzora ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. No u slučaju da je korisnik prekršio pravila sigurnosne politike, ne može se više osigurati povjerljivost informacija otkrivenih u istrazi, te se one mogu koristiti u stegovnom ili sudskom postupku.

**Članak 28.**

Korisnici su dužni pomoći osobama zaduženim za nadzor informacijskih sustava, na taj način što će im pružiti sve potrebne informacije i omogućiti im pristup prostorijama i opremi radi provođenja nadzora.
Isto vrijedi i za administratore računala i pojedinih servisa, koji su dužni specijalistima za sigurnost pomagati pri istrazi.
Pristup uključuje:

- pristup na razini korisnika ili sustava svoj računalnoj opremi,
- pristup svakoj informaciji, u elektroničkom ili tiskanom obliku, koja je proizvedena ili spremljena na opremi Sveučilišta ili oprema Sveučilišta služi za njezin prijenos,
- pristup radnom prostoru (uredu, laboratoriju, sigurnoj zoni itd.),
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Fakulteta.

**Članak 29.**

Zaposlenika koji se ogluši na pravila o nadzoru može se disciplinski kazniti ili mu uskratiti prava korištenja CARNetove mreže i njezinih servisa.

**Rješavanje sigurnosnih incidenata**

**Članak 30.**

Svaki zaposlenik, student ili suradnik Sveučilišta dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.
Voditelj SIC-a, tj. voditelji informatičkih službi sastavnica, trebaju izraditi i održavati kontakt listu osoba kojima se prijavljuju problemi u radu mreže, mrežnih servisa i mrežne opreme, te obrazac za prijavu incidenta. Kontakt listu treba podijeliti svim zaposlenima i objaviti je na internim web stranicama Sveučilišta, tj. sastavnice.
Svaki incident se dokumentira. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac s opisom incidenta i poduzetih mjera pri rješavanju problema.

**Članak 31.**

Izvještaji o incidentima smatraju se povjerljivim dokumentima, spremaju se na sigurno mjesto i čuvaju 10 godina, kako bi mogli poslužiti za statističke obrade kojima je cilj ustanoviti najčešće propuste radi njihova sprečavanja, ali isto tako i kao dokazni materijal u eventualnim stegovnim ili sudskim procesima.
Ozbiljniji incidenti prijavljuju se CARNetovom CERT-u, preko obrasca na web stranici www.cert.hr

**Članak 32.**

Administratori smiju pratiti korisničke procese, ako sumnjaju da se računalo koristi na nedozvoljen način, mogu izlistati sadržaj korisničkog direktorija, ali ne smiju provjeravati sadržaj korisničkih podatkovnih datoteka (na pr. dokumenata ili e-mail poruka).
Daljnju istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost, uz poštivanje slijedećih pravila:

- istragu provodi jedna osoba, ali uz prisustvo svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama,
- prvo pravilo forenzičke istrage jest da se informacijski sustav sačuva u zatečenom stanju, odnosno da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje,
- neophodno je napraviti kopiju zatečenog stanja (npr. na traku, CD, HDD...), po mogućnosti na takav način da se ne izmijene atributi datoteka,
- dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage,
- o istrazi se napiše izvještaj, kako bi u slučaju potrebe mogli poslužili kao dokaz u eventualnim stegovnim ili sudskim procesima,
- izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlaštene osobe.

Sveučilište može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

**Članak 33.**

Svrha je istrage da se odredi uzrok nastanka problema, te da se iz toga izvuku zaključci o tome kako spriječiti ponavljanje incidenta, ili se barem bolje pripremiti za slične situacije. Ako je uzrok sigurnosnom incidentu bio ljudski faktor, protiv odgovornih se mogu poduzeti sankcije.
Sveučilište može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima. Ukoliko je incident izazvao zaposlenik vanjske tvrtke, Sveučilište može zatražiti od vanjske tvrtke da ga ukloni sa liste osoba ovlaštenih za obavljanje posla na ustanovi. U slučaju teže povrede pravila sigurnosne politike, Sveučilište može raskinuti ugovor s vanjskom tvrtkom.

**Prijelazne i završne odredbe**

**Članak 34.**

Ovaj Pravilnik o sigurnosti informacijskih sustava Sveučilišta u Rijeci stupa na snagu osmog dana od dana objave na oglasnoj ploči Sveučilišta u Rijeci.

REKTOR
prof. dr. sc. Pero Lučin

Pravilnik o sigurnosti informacijskih sustava je objavljen na oglasnoj ploči dana 10. ožujka 2015. godine i stupio je na snagu dana 17. ožujka 2015. godine.

U Rijeci, 17. ožujka 2015. godine

GLAVNA TAJNICA
Roberta Hlača Milinar, dipl. iur.